Warszawa, 24 grudnia 2018 roku

Do wszystkich Wykonawców

Dotyczy: ***„Dostawa Systemu stanowiącego Infrastrukturę bezpieczeństwa OSE w ramach projektu Budowa Ogólnopolskiej Sieci Edukacyjnej."***

znak postępowania: **ZZ.2131.519.2018.MWI [OSE-S] [OSE-B] [OSE2019]**

WYJAŚNIENIE TREŚCI ZAPYTANIA OFERTOWEGO

I. Zgodnie z Rozdziałem VII pkt 7 Zapytania ofertowego, Zamawiający przekazuje poniżej pytania Wykonawców dot. treści Zapytania ofertowego wraz z wyjaśnieniami Zamawiającego:

Pytanie nr 189:

1.Dotyczy Załącznik nr 1 do OPZ. Zamawiający wymaga zapewnienia infrastruktury 2 Centralnych Węzłów Bezpieczeństwa dla lokalizacji Warszawa i Poznań. Na mapie na str. 16 prezentującej topologię przedstawione są kolorem fioletowym 3 Węzły Centralne. Czy 3-ci z Węzłów Centralnych ma nie posiadać infrastruktury bezpieczeństwa przewidzianej dla 2 sztuk Centralnych Węzłów Bezpieczeństwa o których Zamawiający wspomina ?

Odpowiedź nr 189:

Na mapie podanej na stronie 16 są wyszczególnione Węzły Centralne. Zgodnie z opisem Węzłów Centralnych na str 14 jedynie w dwóch Węzłach Centralnych będą zainstalowane Centralne Węzły Bezpieczeństwa, w związku z czym Wykonawca nie musi dostarczać urządzeń realizujących funkcje Centralnego Węzła Bezpieczeństwa do trzeciego Węzła Centralnego.

Pytanie nr 190:

2. Dotyczy Załącznik nr 1 do OPZ pkt. 3 , str. 18. Prosimy o wyjaśnienie co wdg. Zamawiajacego oznacza wymaganie w brzmieniu: "Jednocześnie proponowane rozwiązania dla poszczególnych węzłów powinny być zunifikowane." ? Czy oznacza to, że jeśli dla jednego typu RWB kalkulacja wskaże, iż wymagania techniczno-kosztowe najlepiej spełnia rozwiązanie klasy blade a dla innego węzła RWB rozwiązanie bazujące na architekturze stand-alone (nie blade) to będzie to uznane przez Zamawiającego jako rozw zunifikowane spełniające wymagania ?

Odpowiedź nr 190:

Poprzez sformułowanie, ze „proponowane rozwiązania dla poszczególnych węzłów powinny być zunifikowane" Zamawiający ma na myśli dostarczenie przez Wykonawcę jak najmniej rożnych modeli urządzeń. Sytuacja wskazana przez Wykonawcę, tzn. zastosowanie rozwiązania klasy blade i klasy stand-alone, jest sytuacją dopuszczalną ze strony Zamawiającego.

Pytanie nr 191:

3.Dotyczy Załącznik nr 1 do OPZ pkt. 3.2.2 , str. 22. Zamawiający pisze: "Po dokonaniu deszyfracji, cały ruch zostanie przekierowany do Systemu NG Firewall, gdzie będą zdefiniowane polityki dotyczące ruchu warstwy

---

3/4 i uruchomione zostaną funkcjonalności IPS (100% ruchu), AV (9% ruchu - inspekcji AV będzie podlegał ruch niezwiązany z ruchem webowym HTTP/HTTPS) i Kontroli aplikacji (100% ruchu). W przypadku kiedy będzie to żądanie do serwisów web (HTTP, HTTPS), System przekieruje cały taki ruch do Systemu SWG." Zwracamy się z prośbą o wyjaśnienie czy wymaganie to oznacza, że ruch typu WEB (nie szyfrowany i rozszyfrowany) ma w pierwszym kroku zostać przetworzony przez NG Firewall i następnie przekierowany do systemu SWG, czy też w przypadku ruchu WEB NG Firewall jest pominięty na ścieżce ruchu w wyniku przekierowania go bezpośrednio z ADC do SWG (z pominięciem w tym procesie NG Firewall)?

Odpowiedź nr 191:

Zamawiający wymaga aby zaimplementowana inżynieria ruchu powodowała, ze ruch WEB przejdzie w pierwszej kolejności przez NG Firwall, a następnie zostanie przekierowany do systemu SWG.

Pytanie nr 192:

4. Dotyczy Załącznik nr 1 do OPZ pkt. 3.3 , str. 25. Zamawiający w tabeli prezentuje ilość miejsca w szafach rack (w jednostkach „U") oraz dostępną moc (kW) dla poszczególnych Węzłów. Prosimy o wyjaśnienie czy:

- dane tabelaryczne obejmują tylko węzły RWB czy również Centralne Węzły Bezpieczeństwa (CWB) a jeśli i CWB to jakie są parametry dla węzłów centralnych gdzie mają być instalowane urządzenia bezpieczeństwa?

- czy dopuszczone zostanie rozwiązanie przekraczające ilość jednostek „U" i przyznaną moc w przypadku jeśli wymagania jakie postawił by Zamawiający będą skutkowały przekroczeniem wskazanych wartości (jeśli tak prosimy o informacje czy wystarczające będzie dostarczenie dodatkowych szaf rack i ewent. rozbudowa systemu zasilania gwarantowanego w oparciu o informacje o aktualnych parametrach systemu zasilania w danym RWB) ?

Odpowiedź nr 192:

podpunkt 1

W przypadku węzłów znajdujących się w Warszawie i w Poznaniu, parametry podane w tabeli należy rozumieć jako sumaryczną wartość potrzebną do instalacji RWB i CWB.

Podpunkt 2

Zamawiający odrzuci takie rozwiązanie jako nie spełniające wymagań określonych w Szczegółowym opisie przedmiotu zamówienia.

Pytanie nr 193:

5. Dotyczy Załącznik nr 1 do OPZ pkt. 3.5 b) , str. 33. Czy w ramach klastrowania elementów bezpieczeństwa przy oferowaniu urządzeń nie pracujących ww arch. blade dopuszczalne jest oferowanie architektury gdzie N=1 czyli co najmniej 2 urządzeń przy zachowaniu wymogu zapewnienia zasobów w przypadku awarii na poziomie co najmniej 80% wydajności bazowej czy też wymaganie to oznacza, iż minimalna konfiguracja klastra musi składać się z co najmniej 3 urządzeń i to nawet w przypadku jeśli jedno urządzenie poryje w czasie trwania awarii wymaganą wydajność w danym RWB ?

Odpowiedź nr 193:

W sytuacji opisanej przez Wykonawcę Zamawiający wymaga zastosowania 2 urządzeń.

Pytanie nr 194:

6. Dotyczy Załącznik nr 1 do OPZ pkt. 3.5 c) , str. 33. Czy Zamawiający potwierdza, że wymaganie to (w zakresie wyłączenia) dotyczy również również oferowanego środowiska testowego/LAB ?

Odpowiedź nr 194:

Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 67.

Pytanie nr 195:

7 Dotyczy Załącznik nr 1 do OPZ pkt 3 6 2 1 , str 36 Zamawiający pisze: „Zamawiający dopuszcza realizację tej funkcjonalności w sposób równoważny z wykorzystaniem dedykowanych Urządzeń lub jedynie w Węzłach Centralnych przy założeniu realizacji funkcjonalności AV dla wszystkich Użytkowników obsługiwanych przez dany Węzeł." Prosimy o potwierdzenie, że Zamawiający akceptuje rozwiązanie, w którym kontrola AV dla danego RWB dla typowej pracy węzła RWB (nie w trybie awarii) jest realizowana nie lokalnie w tym że RWB, lecz w jednym z 2 CWB gdzie zlokalizowana będzie infrastruktura bezpieczeństwa przewidziana dla CWB i że w związku z tym Zamawiający zapewni niezbędne pasmo w swojej infrastrukturze sieciowej jak i mechanizmy inżynierii ruchu by ruch przewidziany do inspekcji AV przesłać z RWB do CWB i po dokonaniu inspekcji odesłać z powrotem do danego RWB.

Odpowiedź nr 195:

Zamawiający nie zapewni pasma w swojej infrastrukturze sieciowej dla rozszytego ruchu AV pomiędzy RWB i CWB. W przypadku centralizacji funkcjonalności AV konieczne jest przesłanie 9% ruchu normalnie podlegającego analizie AV w RWB na oddzielnym VLAN'ie i dokonanie inspekcji AV w CWB z uwzględnieniem wykonania dekrypcji i enkrypcji ruchu SSL/TLS, w tymze CWB.

Pytanie nr 196:

8. Dotyczy Załącznik nr 1 do OPZ pkt. 3.6.4 y) , str. 43. Zamawiający pisze: „Tworzonych przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 3.6.4 ppkt. m". Prosimy o wyjaśnienie czy Zamawiający ma na myśli .6.4 ppkt q (fonetycznie: ku)) ?

Odpowiedź nr 196:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 68.

Pytanie nr 197:

9. Dotyczy Załącznik nr 1 do OPZ pkt. 3.6.4 ee) , str. 44. Prosimy o wyjaśnienie czy w świetle tak brzmiącego wymagania Zamawiający nie wymaga by rozwiązanie ADC i SSL komunikowały się z wykorzystaniem dynamicznych prot. routingu np. BGP lub OSPF?

Odpowiedź nr 197:

Zamawiający wymaga wykorzystania routingu dynamicznego w oparciu o BGP lub OSPF. Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 69.

Pytanie nr 198:

10. Dotyczy Załącznik nr 1 do OPZ pkt. 3 6.5 k) , str. 45. Prosimy o wyjaśnienie czy system ma realizować mechanizm wyjątków poprzez statyczną listę kategorii jak opisuje to w tym miejscu Zamawiający i jednocześnie realizować wymaganie dotyczące wyjątków w oparciu o kategoryzacje treści w rozwiązaniu opisanym w pkt. 3 6.3 w pkt t), u), v) w oparciu o mechanizm opisany w pkt. 3.2.2 na str. 22 gdzie Zamawiający stawiał wymaganie w brzmieniu : „Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI i CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii do jakiej należy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS. Wykonawca na etapie realizacji przedmiotu zamówienia jest zobowiązany do konfiguracji Systemu ADC i Systemu DNS w sposób umożliwiający wykonanie tej funkcjonalności." ? Wymaganie statycznej listy wydaje się duplikacją mechanizmu kategoryzacji w odniesieniu do tego obszaru.

Odpowiedź nr 198:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 70.

Pytanie nr 199:

11. Dotyczy Załącznik nr 1 do OPZ pkt. 3.6.5 o), str 45 i 3.7.7 o) str. 64. W świetle tak postawionego wymagania prosimy o podanie nazwy/wersji rozwiązania PKI jakim dysponuje Zamawiający celem ustalenia czy oferowane rozwiązanie będzie spełniać ten wymóg.

Odpowiedź nr 199:

Zamawiający wymaga aby urządzenie inspekcji ruchu ssl/tls umozliwiało na generowania CSR dla SUB CA. Wygenerowany CSR zostanie podpisany przez CA Zamawiającego.

Pytanie nr 200:

12. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7 2 1 , str. 49. Zamawiający pisze „W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa" . Prosimy o wyjaśnienie czy pisząc w/w zdaniu o Regionalnym Węźle Bezpieczeństwa Zamawiajacy ma na myśli Centralny Węzel Bezpieczeństwa? Jednoczesnie Zamawiający pisze poniżej „Zamawiający wymaga aby funkcjonalność AV działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.". Czy Zamawiający pisząc o pkt. 3.3 nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 200:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 71.

Pytanie nr 201:

13. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7.2 2 , str. 50. Zamawiający pisze : „Zamawiający wymaga aby funkcjonalność IPS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 201:

Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 72.

Pytanie nr 202:

14. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7.2.3 , str. 51. Zamawiający pisze : „Zamawiający wymaga aby funkcjonalność Kontroli aplikacji (udostępniona poprzez sieć internet) działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 202:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 73.

Pytanie nr 203:

15. Dotyczy Załącznik nr 1 do OPZ pkt 3.7.3 , str 51. Zamawiający pisze : „Zamawiający wymaga aby System inspekcji DNS działał w skali całego ruchu określonego w punkcie 3.3". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 203:

Zamawiający zdefiniował wymagania na system DNS w skali całego systemu. Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 204:

16. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7.4 , str. 54. Zamawiający pisze : „Zamawiający wymaga aby System ADC działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 204:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 74.

Pytanie nr 205:

17. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7.5 , str. 57. Zamawiający pisze : „Zamawiający wymaga aby funkcjonalność SSL VPN działała dla liczby użytkowników określonej w punkcie 3.3.". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 205:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 75.

Pytanie nr 206:

18. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7.6 , str. 58. Zamawiający pisze : „Zamawiający wymaga aby Funkcjonalność WAF działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3 ". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 206:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 76.

Pytanie nr 207:

19. Dotyczy Załącznik nr 1 do OPZ pkt. 3.7.7 , str. 63. Zamawiający pisze : „Zamawiający wymaga aby funkcjonalność Inspekcji ruchu SSL/TLS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3" Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3 3 Zamawiający nie ma na myśli wymagań z punktu 3.3.2 ?

Odpowiedź nr 207:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 77.

Pytanie nr 208:

20. Dotyczy Załącznik nr 1 do OPZ pkt. 3.8 , str. 67. Zamawiający pisze : „Wydajność Węzła laboratoryjnego musi być zgodna z tabelą podaną w rozdziale 3.3 ..". Prosimy o wyjaśnienie czy pisząc w/w zdaniu o pkt. 3.3 Zamawiający nie ma na myśli wymagań z punktu 3.3.3 ?

Odpowiedź nr 208:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 78.

Pytanie nr 209:

21. Dotyczy Załącznik nr 1 do OPZ pkt. 3.8.1 , str. 67. Zamawiający pisze: „Wykonawca musi dostarczyć po jednym Urządzeniu z dostarczonych modeli:" i poniżej wymienia modele. Prosimy o wyjaśnienie czy dopuszczalne jest by jedno z urządzeń wymienionych w tym punkcie realizowało więcej niż jedną funkcję naraz (np. ADC i inspekcja SSL/TLS) przy zachowaniu łącznych param. wydajnościowych opisanych w pkt. 3.3.3 dla środowiska laboratoryjnego ?

Odpowiedź nr 209:

Zmawiający nie dopuszcza takiego rozwiązania. Zamawiający podtrzymuje obecne brzmienie zapisów Zapytania ofertowego.

Pytanie nr 210:

22. Dotyczy Załącznik nr 1 do OPZ pkt. 3.8.2 , str. 68. Zamawiający wymaga dostarczenia kompletnego środowiska wirtualnego (serwer wraz z licencjami). Jednocześnie Zamawiający twierdzi, że do modelowania CBD i RWB musi uwzględnić nie mniej niż 30 urządzeń CPE. W związku z powyższym prosimy o wyjaśnienie czy:

- urządzenia CPE jakie dostarczy Zamawiający są zwirtualizowane i mają być emulowane na w/w serwerze a jeśli tak to jakie są wymagania dla pojedyńczej instancji wirtualnego CPE i pod jakim wirtualizatorem musi ona być uruchomiona ?
- oprogramowanie, o którym wspomina Zamawiający w Załączniku nr 1 do OPZ pkt. 3.8.3 , str. 68 i które Zamawiający zamierza dostarczyć będzie również instalowane w formie zwirtualizowanej na wymaganym do dostarczenia przez Wykonawcę serwerze? W przypadku odpowiedzi twierdzącej prosimy o podanie wymaganych fo zapewnienia zasobów sprzętowych pod w/w oprogramowanie (DRAM,CPU,HDD, wirtualizator) jakie powinny być dodatkowo zabezpieczone na oferowanym serwerze.
- Zamawiający może wyjaśnić jakie licencje ma zapewnić wraz z serwerem Wykonawca zgodnie z wymaganiami opisanymi w Załączniku nr 1 do OPZ pkt. 3.8.3 , str. 68 i czy chodzi tu o wrtualizator czy i jakies inne oprogramowanie np. systemy operacyjne jakie miały by być instalowane na wirtualizatorze (prosimy o podanie zarówno wersji systemów operacyjnych bądź wirtualizatorów jak i ilości)
- Zamawiający zapewni wszystkie wymagane licencje na systemy operacyjne bądź aplikacje jakie zamierza Zainstalować na oferowanym przez Wykonawcę serwerze ?
- Zamawiający jako dostawca i właściciel oprogramowania jakie zamierza uruchomić na środowisku wirtualnym może określić jednoznacznie minimalne zasoby sprzętowe jakie winien spełniać oferowany przez Wykonawcę serwer (DRAM, CPU, HDD), typ i wersja wirtualizatora ?
- serwer jaki ma być dostarczony w ramach środowiska wirtualnego może być wykorzystany do instalacji wirtualnych wersji komponentów środowiska węzła laboratoryjnego w przypadku jeśli Wykonawca zaoferował by część z komponentów przedstawionych w pkt. 3.8.1 w postaci zwirtualizowanej w miejsce urządzeń fizycznych (appliances) ?
- oferowany serwer służyć ma wyłącznie dla celu uruchomienia komponentów systemu laboratoryjnego czy też moze on zostać wykorzystany do instalacji innych komponentów np. wersji programowych centralnych systemów zarządzania poszczególnymi produktami bezpieczeństwa instalowanymi w RWB i CWB?

Odpowiedź nr 210:

Podpunkt 1:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 45, opublikowana w dniu 20.12.2018 r.

Podpunkt 2:
Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 79

Podpunkt 3 i 4 i 5:
Dostarczenie środowiska wirtualnego w ramach Węzła laboratoryjnego jest w pełni po stronie Wykonawcy.

Podpunkt 6:
W pkt 3.8.1 Szczegółowego opisu przedmiotu zamówienia Zamawiający wymaga dostarczenia urządzeń fizycznych w związku z czym Zamawiający nie akceptuje takiego rozwiązania.

Podpunkt 7:
Zamawiający posiada dedykowane środowisko wirtualne, na którym Wykonawca będzie mógł uruchomić oferowany produkcyjny System zarządzający.

Pytanie nr 211:

23. Dotyczy Załącznik nr 1 do OPZ pkt. 3.9.1 pkt. q (fonet. 'ku'), str. 69. Czy Zamawiający potwierdza, iż w przypadku jeśli Wykonawca przewiduje do zastosowania pod komponenty systemów centralnego zarządzania rozwiązania programowe(wirtualne) w miejsce fizycznych (sprzętowych) to Zamawiający zapewni we własnym zakresie niezbędne serwery wraz z oprogramowaniem (wirtualizator, systemy operacyjne itp.) dla instalacji oprogramowania Wykonawcy ?

Odpowiedź nr 211:

Zamawiający zapewni we własnym zakresie niezbędne serwery wraz z oprogramowaniem dla instalacji oprogramowania Wykonawcy w zakresie instalacji Systemu zarządzającego.

Pytanie nr 212:

24. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10.2. Zamawiający stawia wymaganie odnośnie integracji Systemu z systemem provisioningu dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy (w okresie 12 miesięcy od podpisania umowy zgodnie z Załączniku nr 2 do OPZ par. nr 8) z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 i par. nr 8 . Czy Zamawiający posiada juz wspomniany system provisioninu a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie systemu provisioningu i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy system provisioningu będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z systemem provisioningu.

Odpowiedź nr 212:

Zamawiający nie posiada jeszcze systemu provisioningu. Zamawiający planuje rozpoczęcie procesu integracji systemu provisioningu z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 213:

25. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10.3. Zamawiający stawia wymaganie odnośnie integracji oferowanego Systemu z Systemem Fault Management dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy (w okresie 12 miesięcy od podpisania umowy zgodnie z Załączniku nr 2 do OPZ par. nr 8) z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 i par. nr 8. Czy Zamawiający posiada już wspomniany System Fault Management a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie Systemu Fault Management i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy System Fault Management będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z Systemem Fault Management.

Odpowiedź nr 213:

Zamawiający nie posiada jeszcze systemu Fault Management. Zamawiający planuje rozpoczęcie procesu integracji systemu Fault Management z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 214:

26. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10.4. Zamawiający stawia wymaganie odnośnie integracji oferowanego Systemu z Systemem Performance Management dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 . Czy Zamawiający posiada już wspomniany System Performance Management wraz z aktywnym wsparciem producenta rozwiązania a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie Systemu Performance Management i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy System Performance Management będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z Systemem Performance Management.

Odpowiedź nr 214:

Zamawiający nie posiada jeszcze systemu Performance Management. Zamawiający planuje rozpoczęcie procesu integracji systemu Performance Management z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 215:

27. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10.5. Zamawiający stawia wymaganie odnośnie integracji oferowanego Systemu z Systemem Inventory dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy (w okresie 12 miesięcy od podpisania umowy zgodnie z Załączniku nr 2 do OPZ par nr 8) z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 i par. nr 8 . Czy Zamawiający posiada już wspomniany System Inventory wraz z aktywnym wsparciem producenta rozwiązania a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie Systemu Inventory i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy System Inventory będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z Systemem Inventory.

Odpowiedź nr 215:

Zamawiający nie posiada jeszcze systemu Inventory. Zamawiający planuje rozpoczęcie procesu integracji systemu Inventory z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 216:

28. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10.6. Zamawiający stawia wymaganie odnośnie integracji oferowanego Systemu z Systemem Config Management dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy (w okresie 12 miesięcy od podpisania umowy zgodnie z Załączniku nr 2 do OPZ par. nr 8) z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 i par. nr 8 . Czy Zamawiający posiada już wspomniany System Config Management a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie Systemu Config Management i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy System Config Management będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z Systemem Config Management.

Odpowiedź nr 216:

Zamawiający nie posiada jeszcze systemu Config Management. Zamawiający planuje rozpoczęcie procesu integracji systemu Config Management z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 217:

29. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10 7. Zamawiający stawia wymaganie odnośnie integracji oferowanego Systemu z Systemem SWG dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy (w okresie 12 miesięcy od podpisania umowy zgodnie z Załączniku nr 2 do OPZ par. nr 8) z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 i par. nr 8. Czy Zamawiający posiada już wspomniany System SWG a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie Systemu SWG i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy System SWG będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z Systemem SWG

Odpowiedź nr 217:

Zamawiający nie posiada jeszcze systemu SWG. Zamawiający planuje rozpoczęcie procesu integracji systemu SWG z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 218:

30. Dotyczy Załącznik nr 1 do OPZ pkt. 3.10.8. Zamawiający stawia wymaganie odnośnie integracji oferowanego Systemu z Systemem SIEM dodatkowo stawiając Wykonawcy wymagania w zakresie pełnej i praktycznie nie limitowanej czasem i zakresem współpracy (w okresie 12 miesięcy od podpisania umowy zgodnie z Załączniku nr 2 do OPZ par. nr 8) z dostawcami rozwiązań Zamawiającego poprzez zapisy zawarte w Załączniku nr 2 do OPZ, wzór umowy par.2 pkt. 4 i par. nr 8 . Czy Zamawiający posiada już wspomniany System SIEM a jeśli tak to prosimy o podanie nazwy produktu i wersji realizującego w/w funkcje? Jeśli Zamawiający nie posiada obecnie Systemu SIEM i planuje go zaimplementować w swojej infrastrukturze prosimy o podanie daty od kiedy System SIEM będzie w stanie operacyjnym umożliwiającym podjęcie działań zmierzających do integracji oferowanych w postępowaniu komponentów Systemu z Systemem SIEM.

Odpowiedź nr 218:

Zamawiający nie posiada jeszcze systemu SIEM. Zamawiający planuje rozpoczęcie procesu integracji systemu SIEM z dostarczaną przez Wykonawcę Infrastrukturą bezpieczeństwa w II kwartale 2019 r.

Pytanie nr 219:

31. Dotyczy Załącznik nr 2 do OPZ, wzór umowy par.1, Definicje pkt. 40. Zamawiający definiuje pojęcie Usługi odnosząc się do załącznika 12. Załącznik 12 zawiera Opis testów weryfikacyjnych. Prosimy o wyjaśnienie jak definicja Usługi powiązana jest z załącznikiem nr 12 lub wskazanie do jakiego innego załącznika ma ona się odwoływać.

Odpowiedź nr 219:

Zamawiający wyjaśnia, że zgodnie z zapisami Wzoru Umowy (załącznik nr 2 do Zapytania Ofertowego) definicja w pkt 40 dotyczy Utrzymania. Załącznik nr 12 do Umowy dotyczy zakresu Utrzymania. Załącznik nr 12 do Zapytania Ofertowego zawiera Opis testów weryfikacyjnych.

Pytanie nr 220:

32. Dotyczy Załącznik nr 2 do OPZ, wzór umowy par.1 . Zamawiający w niniejszym paragrafie zawiera poszczególne definicje. Prosimy o wyjaśnienie jak zostanie zinterpretowana sytuacja uszkodzenia jednego z komponentów systemu w RWB bądź CWB jeśli w jej wyniku zachowany jest poziom wydajności rozwiązania w danej lokalizacji na poziomie co najmniej 80% a uszkodzenie nie wpływa w inny sposób negatywnie na architekturę rozwiązania? Czy w świetle tak opisanej sytuacji uszkodzenie takie będzie traktowane jako „Awaria" czy też „Błąd i Wada" ? Z definicji „Awarii Krytycznej" wynika, iż wydajność obniżona o co najmniej 20% (czyli realna wydajność spada poniżej 80%) jest klasyfikowana jako „Awaria Krytyczna" jednak brak jest jednoznacznego opisu jak będzie klasyfikowane zdarzenie wchodzące w podzbiór definicji należących do

---

zdarzenia opisanego jako „Problem" przy zaistnieniu sytuacji degradacji wydajności węzła RWB/CWB mniejszej niż 20%.

Odpowiedź nr 220:
W przypadku wystąpienia Problemu i zachowania wydajności Systemu na poziomie nie mniejszym niz 80% Zamawiający skwalifikuje dany Problem jako Awarię. W przypadku degradacji wydajności większej niz 20% Zamawiający zgłosi Problem skategoryzowany jako Awaria Krytyczna.

Pytanie nr 221:
33. Dotyczy Załącznik nr 7 do OPZ, Zamawiający w pkt. Nr 3 wymaga przeprowadzenia „Instruktazu zaawansowanego" a jak wynika z pkt 3.2 p-pkt. d) również „Instruktażu podstawowego" dla każdego z rozwiązań użytych do budowy Systemu jednak nie definiuje zakresu owych instruktaży tak jak robi to dla Instruktażu w zakresie zastosowanych rozwiązań projektowych i Instruktażu w zakresie dodatkowym opisanych odpowiednio w p-pkt. 2.1 i p-pkt. 2.2. Samo pojęcie „Instruktażu zaawansowanego" jak i „Instruktazu podstawowego" nie zostaje nigdzie jednoznacznie zdefiniowane. W związku z powyższym zwracamy się z uprzejmą prośbą o wyjaśnienie jaki zakres tematyczny jest przewidziany do realizacji Instruktażu zaawansowanego i czym zakres ten ma różnić się od instruktażu podstawowego o ile taki również ma być prowadzony dla wymienionych w pkt. a-f) rozwiązań. Jednocześnie Zamawiający wymaga by oba instruktaże z pkt. 3 odbyły się w autoryzowanych ośrodkach szkoleniowych w związku z tym prosimy o udzielenie odpowiedzi czy instruktaże te mają mieć status nie autoryzowanych szkoleń (warsztatów) czy też mają być to szkolenia autoryzowane na warunkach jakie narzuca producent autoryzowanemu ośrodkowi szkoleniowemu.

Odpowiedź nr 221:
Zgodnie z zapisami Wzoru Umowy (załącznik nr 2 do Zapytania Ofertowego), załącznik nr 7 do Wzoru Umowy, Instruktaż opisany w pkt. 3 musi być przeprowadzony w ośrodku autoryzowanym przez producenta dostarczonych w ramach realizacji Umowy Urządzeń. Zamawiający nie precyzuje zakresu Instruktazu z pkt.3 gdyz zalezeć on będzie od zaoferowanego przez Wykonawcę Systemu.

Pytanie nr 222:
34. Dotyczy Załącznik nr 8 do OPZ, p-pkt 2.3.3 Czy Zamawiający zgodzi się na wydłużenie czasu na podjęcie prac konsultacji z aktualnie zapisanego, absurdalnie krótkiego 2 godzinnego czasu ich podjęcia? Zwracamy uwagę, że konsultacje te nie są sytuacją związaną z awarią systemu bądź jego komponentów w związku z tym w żadnym wypadku nie zachodzi potrzeba realizacji takich działań w trybie SLA zbliżonego dla sytuacji definiowanej jako awaria krytyczna. Zwracamy uwagę, ze zakres technologii jakich dotyczy wymaganie konsultacji jest tak szeroki, że może skutkować koniecznością stałego utrzymania zespołu wysoko kwalifikowanych inżynierów wyłącznie dla zapewnienia 2 godzinnego czasu obsługi zgłoszenia konsultacji uniemożliwiając im świadczenie normalnych prac wdrożeniowo serwisowych w ramach ich obowiązków co z kolei wygeneruje znacznie wyższe koszty świadczenia usługi jaką wymaga Zamawiający. W ocenie Wykonawcy rozsądny termin dla realizacji analogicznych zleceń konsultacji praktykowany w innych przypadkach wynosi kilka dni roboczych przy czym dokładny termin świadczenia usługi jest ustalany z chwilą zgłoszenia takiego wniosku (wraz z podstawowym zakresem tematycznym) pomiędzy Zamawiającym i Wykonawcą tak by zapewnić rozsądne dysponowanie zasobami ludzkimi po obu stronach. Wymaganie konsultacji z 2 godzinnym czasem na podjęcie świadczenia nosi znamiona usługi help-line świadczonej zwykle przez serwisy producentów czyli zupełnie innej usługi wsparcia niż usługi konsultacji.

Odpowiedź nr 222:
Zmawiający informuje, ze przez "czas podjęcia obsługi" należy rozumieć czas rozpoczęcia obsługi konsultacji a nie czas zakończenia konsultacji.
Zamawiający pozostaje przy obecnym brzmieniu zapisów Zapytania ofertowego.

Pytanie nr 223:
35 Dotyczy Załącznik nr 12 do OPZ, p-pkt 1.4. Czy Zamawiający potwierdza, że odwzorowanie środowiska testowego dla RWB woj. Opolskiego dotyczy również redundancji jak i pełnego odwzorowania liczby poszczególnych komponentów zastosowanych dla implementacji węzła RWB Opole ?

Odpowiedź nr 223:

Zamawiający wymaga aby Wykonawca odwzorował w pełnym zakresie wydajnościowym i funkcjonalnym RWB Opole. Zamawiający nie wymaga dostarczenia Urządzeń redundantnych.

Pytanie nr 224:

36. Dotyczy Załącznik nr 12 do OPZ. Zamawiający w dokumencie posługuje się pojęciem CPS. Prosimy o wyjaśnienie w której warstwie sieciowej mają być mierzony wspomniany parametr CPS? Zwracamy uwagę że Zamawiający posługiwał się w Zał. nr 1 pojęciem „New CPS" które zostało zdefiniowane.

Odpowiedź nr 224:

Zamawiający traktuje tak samo zapisy "CPS" w Załączniku nr 12 do Zapytania ofertowego jak "New CPS" w Załączniku nr 1 do Zapytania ofertowego.

Pytanie nr 225:

37. Dotyczy Załącznik nr 1 do OPZ. Zamawiający definiuje pojęcie: „Persistent connection". Prosimy o uszczegółowienie czy dotyczy ono warstwy 4-ej czy siódmej ?

Odpowiedź nr 225:

Pojęcie „Persistent connection" dotyczy warstwy czwartej.

Pytanie nr 226:

38. Dotyczy Załącznik nr 1 do OPZ, pkt. 3. Prosimy o wyjaśnienie czy Zamawiający dopuści rozwiązania, które na dzień składania oferty nie posiadają pewnych wymaganych funkcjonalności (co zostałoby uwzględnione poprzez dokonanie stosownej adnotacji w Załączniku nr 9), ale producent danego rozwiązania zapewni, że zostaną one uzupełnione przed terminem odbioru pierwszej fazy projektu?

Odpowiedź nr 226:

Zamawiający nie dopuszcza takiego rozwiązania. Oferowane przez Wykonawcę rozwiązanie musi posiadać wszystkie wymagane przez Zamawiającego funkcjonalności, opisane w Zapytaniu ofertowym, na dzień składania ofert.

Pytanie nr 227:

39. Dotyczy Załącznik nr 1 do OPZ, pkt. 3 Prosimy o wyjaśnienie czy Zamawiający wymaga aby pełna dokumentacja rozwiązań komercyjnych oferowanych w postępowaniu była dostępna publicznie?

Odpowiedź nr 227:

Zamawiający wymaga, aby dokumentacja rozwiązań oferowanych w postępowaniu była dostępna publicznie.

Pytanie nr 228:

40. Dotyczy Załącznik nr 1 do OPZ, pkt. 3. Zamawiający wymaga dla Systemów ADC i NG Firewall zaoferowania rozwiązań uwzględnionych w raportach branżowych takich jak Magic Quadrant Gartnera. Czy w związku z tym analogicznie zaoferowane rozwiązanie dla Systemu DNS musi opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Market Guide for DNS, DHCP and IP Address Management (DDI), lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich dwóch lat?

Odpowiedź nr 228:

Zamawiający nie wymaga aby producent Systemu DNS był uwzględniony w wymienionych przez Wykonawcę zestawieniach.

Pytanie nr 229:

41. Dotyczy Załącznik nr 1 do OPZ pkt. 3.6.4 o-p) i pkt. 3.6.5 q-r) str. 44. Czy Zamawiający zgodzi się na realizacje wymagań w zakresie kategoryzacji (na poszczególnych systemach, których dotyczą w/w wymagania) poprzez zapewnienie na rozwiązaniu ADC/SSL własnej, globalnej bazy kategoryzacji (bez ponoszenia dodatkowego kosztu po stronie Zamawiającego) tak by nie było konieczności korzystania w tym zakresie z systemu DNS ?

Odpowiedź nr 229:

Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 80.

Pytanie nr 230:

42. Dotyczy Załącznik nr 1 do OPZ pkt. 3.6.4 o-p) i pkt. 3.6.5 q-r) str. 44. Czy Zamawiający zgodzi się na realizacje wymagań w zakresie kategoryzacji (na poszczególnych systemach, których dotyczą w/w wymagania) we współpracy z system DNS w nieco inny sposób tj. z wykorzystaniem bardziej zestandaryzowanego mechanizmu API ?

Odpowiedź nr 230:

Zamawiający nie określa sposobu integracji Systemu DNS i Systemu ADC.

Pytanie nr 231:

43. Dotyczy Załącznik nr 1 do OPZ pkt. 3 7.6 cc) str. 62 . Czy Zamawiający dopuści alternatywną metodę wykrywania botnetów w stosunku do wymagania w zakresie wykorzystywania mechanizmu CAPTCHA (ostatni tiret) w oparciu o mechanizm fingerprinting? Metoda CAPTCHA posiada wiele podatności umożliwiających jej stosunkowo proste obejscie i w związku z powyższym uznawana jest za metodę przestarzałą o ograniczonej skuteczności i współcześnie jest zastępowana znacznie skuteczniejszą metodą fingeprintingu nakierowaną na detekcje botów sterowanych z botnetów.

Odpowiedź nr 231:

Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 62, opublikowana na w piśmie z dnia 20.12.2018r.

Pytanie nr 232:

Czy Zamawiający dopuści, aby zaoferowane rozwiązanie umożliwiało uruchomienie dynamicznych protokołów routingu (RIP, OSPF, BGP) jako opcję i dopuści nie wycenianie w bieżącym postępowaniu licencji umożliwiających ich uruchomienie? Zgodnie z naszą najlepszą wiedzą w projekcie nie ma konieczności uruchamiania dynamicznych protokołów routingu, a złagodzenie tego wymagania umozliwiłaby znaczną optymalizację cenową

Odpowiedź nr 232:

Zamawiający nie dopuści rozwiązania nie wspierającego dynamicznych protokołów routingu. Zamawiający wymaga uruchomienia dynamicznych protokołów routingu (BGP lub OSPF) w ramach realizacji Umowy, której zawarcie będzie wynikiem przeprowadzenia niniejszego postępowania. Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 233:

Pytanie odnosi się do punktu 3.7.6 cc) Czy Zamawiający zgodzi się na dopuszczenie rozwiązania, które zamiast CAPTCHA wykorzystuje mniej podatne na ataki, a przez to znacznie bezpieczniejsze technologie jak np. fingerprinting?

Odpowiedź nr 233:

Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 62, opublikowana w piśmie z dnia 20.12.2018 r.

Pytanie nr 234:
Czy Zamawiający dopuszcza, aby system SSLVPN opisany w rozdziale 3.7.5 umozliwiał konfigurację reguł polityki dostępu opisany w punkcie b) w sposób graficzny, ale definiowanie makr i ich sekwencji w sposób tekstowy?
Odpowiedź nr 234:
Zamawiający dopuszcza definiowanie makr i ich sekwencji w sposób tekstowy z wykorzystaniem graficznego edytora, który Zamawiający utożsamia z interfejsem GUI.
Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 81.

Pytanie nr 235:
Czy Zamawiający dopuści, aby system SSLVPN opisany w rozdziale 3.7.5 w module poprawności aplikacji opisanym w punkcie g) nie obsługiwał sprawdzania CPU ID i HDD ID?
Odpowiedź nr 235:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 57, opublikowana w piśmie z dnia 20.12.2018 r.

Pytanie nr 236:
Czy Zamawiający dopuści, aby system SSLVPN opisany w rozdziale 3.7.5 nie będzie zapewniał Zamawiającemu w procesie logowania opisanym w punkcie o) wirtualnej klawiatury?
Odpowiedź nr 236:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 58, opublikowana w piśmie z dnia 20.12.2018 r.

Pytanie nr 237:
Dot. wymagania 3.6.2.v oraz 3.7.2.v
Czy Zamawiający dopuści rozwiązanie, gdzie w kontekście identyfikacji uzytkownika będzie podawana jego nazwa i przynależność do grupy bez źródłowego adresu IP i nazwy urządzenia?
Odpowiedź nr 234:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 7 i 8, opublikowana w dniu 18.12.2018 r.

Pytanie nr 238:
Dotyczy wymagań na podsystem AV wymienione w rozdziałach m. in. 3.6.2.1.a, d ig i 3.7.2.1.a, d i g
Zgodnie z naszą najlepszą wiedzą w sieciach operatorskich na ogół nie dopuszcza się ruchu SMB w kierunku Internetu. Czy Zamawiający dopuści rozwiązanie, które zapewnia skuteczne skanowanie AV dla protokołów: HTTP, SMTP, POP3, IMAP, FTP,MAPI?
Odpowiedź nr 238:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 9, opublikowana w piśmie z dnia 18.12.2018 r.
Po wprowadzeniu powyższej zmianie wymienione protokoły spełniają wymagania.

Pytanie nr 239:
Dotyczy wymagań na podsystem IPS wymienione w rozdziałach m. in. 3.6.2.2.e, 3.7.2.2.e
Czy Zamawiający jest skłonny do ograniczenia wymagania do sygnatur oraz anomalii protokołów w tym analizy behawioralnej? Porównywanie ruchu z wzorcem jest właściwe dla firewalli aplikacyjnych WAF?
Odpowiedź nr 239:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 10, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 240:
Dot. wymagania 3.7.6.o
Czy Zamawiający dopuści WAF, który dobór sygnatur klasyfikuje w zalezności od rodzaju ataku, a do ochrony specyficznych aplikacji posiada predefiniowane profile?
Odpowiedź nr 240:

Zamawiający dopuści WAF, który dobór sygnatur klasyfikuje w zależności od rodzaju ataku, a do ochrony specyficznych aplikacji posiada predefiniowane profil, jezeli profile są tozsame z grupami opisanymi w punkcie 3.7.6 lit. o) Zapytania ofertowego.

Pytanie nr 241:
Dot. wymagania 3.7.6.v
Czy Zamawiający zrezygnuje z tego wymagania, jeżeli oferowany WAF wykorzystuje mechanizm Machine Learning?
Odpowiedź nr 241:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.
Zamawiający informuje jednocześnie, ze uznaje mechanizm Machine Learning jako jeden z potencjalnych algorytmów.

Pytanie nr 242:
Dot. wymagania 3.7.4.a
Gartner obecnie publikuje wymagania dla ADC, czy Zamawiający zaakceptuje rozwiązanie spełniające wymagania Gartnera, ale nie pojawiające się w poprzednich zestawieniach?
Odpowiedź nr 242:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 11, opublikowana w dniu 18.12.2018 r.
Jednocześnie Zamawiający modyfikuje dodatkowo treść Zapytania – patrz zmiana nr 66.

Pytanie nr 243:
Dot. wymagania 3.7.4.b
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 243:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 12, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 244:
Dot. wymagania 3.7.4.c
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 244:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 13, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 245:
Dot. wymagania 3.7.4.e
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 245:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 246:
Dot. wymagania 3 7.4.f
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 246:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 14, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 247:
Dot. wymagania 3.7.4.g
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 247:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 15, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 248:
Dot. wymagania 3.7.4.h
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 248:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 249:
Dot. wymagania 3.7.4.i
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 249:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 16, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 250:
Dot. wymagania 3.7.4.j
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 250:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 17, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 251:
Dot. wymagania 3.7.4.l
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 251:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 18, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 252:
Dot. wymagania 3.7.4.m
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 252:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 19, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 253:
Dot. wymagania 3.7.4.n
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 253:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 254:
Dot. wymagania 3.7.4.o
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 254:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 20, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 255:
Dot. wymagania 3.7.4.p
Czy Zamawiający jest skłonny usunąć to wymaganie w odniesieniu do węzłów centralnych w celu optymalizacji kosztów?
Odpowiedź nr 255:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 21, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 256:
Dot. wymagania 3.7.4.u
Czy Zamawiający zaakceptuje co najmniej w węzłach centralnych system ADC obsługujący jedynie następujące mechanizmy monitorowania: dns, ftp, http, https, icmp, imap4, l2-detection, mysql, DIAMETER, pop3, radacct, radius, rtsp, sip, sip-tcp, smtp, snmp, snmp-custom, ssh, tcp, tcp-echo, tcphalf, tcpssl, udp, Skrypty shell?
Odpowiedź nr 256:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 257:
Dot. wymagania 3.7.4.w
Czy Zamawiający zaakceptuje co najmniej w węzłach centralnych system ADC obsługujący jedynie następujące mechanizmy przywiązania sesji: Source-IP, Source-IP Hash, Source-IP/Port Hash, Hash Header, Hash Request, Persistent Cookie, Rewrite Cookie, Insert Cookie, Hash Cookie, Embedded Cookie, RADIUS Attribute, SSL Session ID?
Odpowiedź nr 257:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 258:
Dot. wymagania 3.7.4.dd
Czy Zamawiający przewiduje obsługę jumbo frames na ADC? Jeżeli nie to prosimy o usunięcie tego wymagania.
Odpowiedź nr 258:
Zamawiaczy wymaga obsługi Jumbo Frames we wdrożonej wersji Systemu.

Pytanie nr 259:
Dotyczy procedury testowej numer 8.
Czy Zamawiający dopuszcza JSON API w przypadku, kiedy system NGFW jest kontrolowany przez centralny system zarządzania?
Odpowiedź nr 259:
Zamawiający informuje, że dopuszcza uzycie formatu JSON API , kiedy system NGFW jest kontrolowany przez centralny system zarządzania. W Rest API jest używany format wejściowy i wyjściowy w formacie JSON.

Pytanie nr 260:
Dot. §1 pkt 23
Zamawiający jednostronnie wskazuje termin rozpoczęcia wdrożenia Węzła dla konkretnej lokalizacji. Może warto zaproponować termin minimalny?

Czy Zamawiający wyrazi zgodę na zmianę §1 pkt 23 wzoru Umowy poprzez dodanie fragmentu „który nie może być krótszy niż 14 dni roboczych"?

Odpowiedź nr 260:

Zgodnie z zapisami Wzoru Umowy termin wdrożenia danego Węzła wskazywany jest przez Wykonawcę w Szczegółowym Harmonogramie Wdrożenia Węzła oraz "Wykonawca jest zobowiązany do zgłoszenia gotowości do Odbioru Wstępnego Węzła w ciągu 105 dni od wydania Polecenia Wdrożenia Węzła." Dodatkowo zgodnie z Załącznikiem nr 1 (SOPZ) do Zapytania ofertowego, punkt 3.9.3, Zamawiający rezerwuje dla siebie 60 dni na "Przygotowanie Obiektów do instalacji Urządzeń".
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 261:

Dot. §2 ust. 4
Na czym będą polegać prace wykonywane przez pozostałych wykonawców? To Zamawiający powinien odpowiadać za koordynację prac wykonawców. Interoperacyjność Systemu powinna być zapewniona na podstawie odpowiedniego sformułowania zapisów OPZ'ów poszczególnych postępowań.

Odpowiedź nr 261:

W ramach budowy sieć OSE będzie realizowanych, poza zakresem Umowy, wiele innych systemów realizowanych przez wykonawców, wybranych w ramach odrębnych postępowań. Wykonawca będzie zobowiązany do współpracy z wykonawcami realizującymi inne systemy w zakresie realizacji Integracji opisanej w Szczegółowym opisie przedmiotu zamówienia, punkt 3.10.

Pytanie nr 262:

Dot. §3 ust. 6
Wykonawca prosi o zmianę terminu na 2 dni robocze.

Odpowiedź nr 262:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 89.

Pytanie nr 263:

Dot. §3 ust. 26
Wykonawca zwraca się o zmianę postanowienia i nadanie mu brzmienia „W przypadku opóźnienia wykonawcy w realizacji umowy w stosunku do terminów wynikających z umowy z powodu okoliczności leżących po stronie Zamawiającego, terminy realizacji automatycznie ulegają wydłużeniu o wyżej wymieniony okres opóźnienia".

Odpowiedź nr 263:

Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 264:

Dot. §4 ust. 11
Czy intencją Zamawiającego jest zwolnienie wykonawcy z obowiązku zapłaty kary umownej za okres wyznaczony na usunięcie Błędów i Wad? W przypadku odpowiedzi twierdzącej wykonawca prosi o przeredagowanie postanowienia w ten sposób, aby fragment „przez okres wyznaczony na usunięcie Błędów i Wad" zastąpić wyrażeniem „za okres wyznaczony na usunięcie Błędów i Wad".

Odpowiedź nr 264:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 82.

Pytanie nr 265:

Dot. §7 ust. 1
Wykonawca zwraca uwagę, że Zamawiający w ustępie 1 odwołuje się do ustępu 7, który nie zawiera żadnej treści.

Odpowiedź nr 265:

Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 37, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 266:
Dot. §8
Wykonawca prosi o doprecyzowanie, że Zamawiający odpowiada za koordynację prac wszystkich wykonawców.
Odpowiedź nr 266:
Zamawiający potwierdza, że odpowiada za koordynacje prac wszystkich wykonawców. Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 267:
Dot. §9 ust. 4
W praktyce moze dojść do sporu, kto odpowiada za wady ujawnione po dokonanej rozbudowie. Wnosimy więc o zaproponowanie dodatkowej procedury uprzedniej akceptacji przez Wykonawcę ewentualnej rozbudowy?
Odpowiedź nr 267:
Zakres Gwarancji jest ograniczony do Urządzeń i Oprogramowania dostarczonych w trakcie realizacji Umowy, której zawarcie będzie wynikiem rozstrzygnięcia niniejszego postępowania. Zamawiający moze dokonać rozbudowy posiadanej infrastruktury sprzętowej oraz teleinformatycznej w sposób zgodny z dokumentacją techniczną urządzeń dostarczonych przez Wykonawcę w trakcie realizacji Umowy.
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 268:
Dot §9 ust. 7
Wykonawca prosi o wskazanie minimalnego terminu na usunięcie wad w ramach rękojmi (nie krótszy niz 30 dni roboczych) oraz ograniczenie uprawnień z tytułu rękojmi w ten sposób, że odstąpienie od umowy lub żądanie obniżenia ceny przysługuje Zamawiającemu wyłącznie po trzykrotnym bezskutecznym skorzystaniu z uprawnienia do żądania wymiany lub naprawy danego urządzenia w ramach rękojmi.
Odpowiedź nr 268:
Zamawiający zmienia §9 ust. 7 wzoru Umowy.
Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 83.

Pytanie nr 269:
Dot. §17 ust. 4
Wykonawca zwraca uwagę, ze czas gwarancji zgodnie z §9 ust. 2 dla poszczególnych Węzłów jest różny. Jaki wpływ ma to na zwolnienie zabezpieczenia zgodnie z §17 ust. 4?
Czy Zamawiający wyrazi zgodę na zmianę zasad zwolnienia zabezpieczenia w ten sposób, aby 70% zabezpieczenia zostało zwolnione po odbiorze końcowym Systemu, natomiast 30% po upływie okresu Gwarancji?

Odpowiedź nr 269:
Zamawiający informuje, że zgodnie z zapisami z Wzoru Umowy "Okres Gwarancji na System wynosi 5 (pięć lat) i rozpoczyna swój bieg od daty dokonania Odbioru Wstępnego pierwszego Węzła". Oznacza to zakończenie Gwarancji dla wszystkich Węzłów w tym samym czasie, przy czym Okres Gwarancji dla poszczególnych Węzłów jest różny.
Zwolnienie zabezpieczenia następuję po upływie Okresu Gwarancji.
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów.

Pytanie nr 270:
Dot. §18 ust. 3
Wykonawca prosi o wskazanie konkretnego terminu obowiązku poufności, który będzie miał związek z planowanym okresem uzytkowania Systemu.
Odpowiedź nr 270:
Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 84.

Pytanie nr 271:
Dot. §19 ust. 2
Wykonawca zwraca się o wprowadzenie górnych limitów dla naliczania kar umownych za opóźnienie do wysokości 100 tyś. zł.
Odpowiedź nr 271:
Zamawiający informuje, że dokonał modyfikacji zapisów Zapytania ofertowego – patrz zmiana nr 52, opublikowana w piśmie z dnia 20.12.2018 r.

Pytanie nr 272:
Dot. §21 ust. 2
Wykonawca prosi o skrócenie okresu na wykonanie prawa odstąpienia do 30 dni.
Odpowiedź nr 272:
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 273:
Czy dopuszcza się się aby serwery DNS (DNS Cache) udostępniały autorytatywnie wpisy własne wprowadzone przez NASK, bez dedykowanych serwerów autorytatywnych DNS (DNS Authoritative)?
Odpowiedź nr 273:
Zamawiający nie rozdziela funkcjonalności serwerów autorytatywnych DNS od pozostałych funkcjonalności wyszczególnionych dla systemu DNS w pkt. 3.6.3 i 3.7.3 Szczegółowego opisu przedmiotu zamówienia.
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.

Pytanie nr 274:
Jeśli wymagane są dedykowane serwery DNS Authoritative, jaka musi być ich wydajność dla ośrodka centralnego i regionalnego?
Odpowiedź nr 274:
Zamawiający określił w punkcie 3.3 Szczegółowego opisu przedmiotu zamówienia (SOPZ) wydajność Systemu DNS w całej sieci OSE na 200 000 QPS. Zgodnie z odpowiedzią na pytwanie nr 273 powyzej, Zamawiający nie rozdziela funkcjonalności serwerów autorytatywnych DNS od pozostałych funkcjonalności wyszczególnionych dla systemu DNS w pkt. 3.6.3 i 3.7.3 SOPZ.

Pytanie nr 275:

punkt 3.3.1 i punkt 3.2.2	W punkcie 3.3.1 w części „Wymagane skalowanie Systemu ADC" Zamawiający podaje wymaganą przepustowości systemu (parametr "Throughput Systemu ADC [Mbps]"). Jednocześnie w punkcie 3.2.2 przedstawia schemat blokowy przepływy danych przez Regionalny Węzeł Bezpieczeństwa.	Czy Wykonawca prawidłowo interpretuje powyższe informacje, że Zamawiający, tak naprawdę, nie podaje wymaganej przepustowości systemu ADC, a informację i ilości ruchu ze szkół, która dla danego Regionalnego Węzła Bezpieczeństwa pojawi się na „pierwszym wejściu" (patrzą na schemat blokowy) do systemu ADC? I to rolą Wykonawcy, co Zamawiający słusznie zauważył w punkcie 3.2.2 („W wymiarowaniu Urządzeń potrzebnych do realizacji funkcji bezpieczeństwa nalezy wziąć pod uwagę potencjalne wielokrotne przejścia tych samych przepływów przez ten sam blok funkcjonalny [...]), jest dobór właściwego parametru dla przepustowości systemu ADC?

Odpowiedź nr 275:
W wymiarowaniu urządzeń Zmawiający podaje ile ruchu musi być obsłużone przez poszczególne Węzły Bezpieczeństwa. W związku z tym, że sposób implementacji ma bezpośredni wpływ na potrzebną wydajność poszczególnych elementów Infrastruktury Bezpieczeństwa, to rolą Wykonawcy jest dobór właściwego parametru dla przepustowości wszystkich elementów Infrastruktury Bezpieczeństwa.

Pytanie nr 276:
Załącznik nr.9 pkt.3.6.3: Prosimy o potwierdzenie, że Wykonawca może zaproponować rozproszoną architekturą systemu DNS w której część analityczna w tym (antymalware, kategoryzacja stron, cache) są ulokowane w silnikach umieszczonych w Centralnych Węzłach Bezpieczeństwa?
Odpowiedź nr 276:
Zamawiający dopuszcza taki model implementacji Systemu DNS pod warunkiem zastosowania hierachicznej struktury DNS w kazdym Węźle Bezpieczeństwa - resolvery i cache, w kazdym Regionalnym Węźle Bezpieczeństwa i nadrzędne serwery DNS, posiadające zawansowane funkcje wymienione przez Wykonawcę, zainstalowane w dwóch Centralnych Węzłach Bezpieczeństwa.

Pytanie nr 277:
Załącznik nr.9 pkt.3.4 s) Wymagania wspólne dla wszystkich elementów Infrastruktury bezpieczeństwa, Prosimy o potwierdzenie, ze dla wymagań firewall w węźle regionalnym wymaganie dotyczy funkcjonalności obejmującej takze NetFlow-v5/9/10/IPFIX na urządzeniu Firewall w RWB.
Odpowiedź nr 277:
Zamawiający informuje, ze nie wymaga funkcjonalności NetFlow-v5/9/10/IPFIX na urządzeniu Firewall w RWB.

Pytanie nr 278:
Załącznik nr.9 pkt.3.6.2 k) Wymaganiami dla Firewall Regionalnego Węzła bezpieczeństwa - prosimy o potwierdzenie, że dla wymagań firewall w węźle regionalnym wymaganie dotyczy standard 802.1Q wraz z Jumbo Frame min. 9000B.
Odpowiedź nr 278:
Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 85.

Pytanie nr 279:
Załącznik nr.9 pkt. 3.6.2.2 f) i 3.7.2.2 f) Nowoczesne systemy firewall dokonują analizy danych strumieniowo (w przeciwieństwie do starych modeli typu proxy) w takiej sytuacji to wymaganie ich nie dotyczy, ponieważ w dokumentacji producenta nie ma o tym mowy prosimy o modyfikację wymagania „Funkcjonalność IPS musi dobierać optymalny mechanizm defragmentacji i składania strumienia danych w zalezności od charakterystyki hosta docelowego DPI, dla trybu pracy proxy."
Odpowiedź nr 279:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 53, opublikowana w piśmie z dnia 20.12.2018 r .

Pytanie nr 280:
Załącznik nr.9 pkt. 3.6.2.1 h) i 3.7.2.1. h) Nowoczesne systemy firewall dokonują analizy danych strumieniowo (w przeciwieństwie do starych modeli typu proxy) w takiej sytuacji to wymaganie ich nie dotyczy, ponieważ w dokumentacji producenta nie ma o tym mowy prosimy o modyfikację wymagania „Funkcjonalność AV musi umożliwiać Zamawiającemu na definiowanie wielkości pliku powyzej, którego funkcjonalność AV nie będzie przeprowadzała inspekcji danego pliku, dla trybu pracy proxy."
Odpowiedź nr 280:
Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 24, opublikowana a piśmie z dnia 18.12.2018 r.

Pytanie nr 281:
Załącznik nr.9 pkt. 3.4.g Czy zamawiający dopuszcza uwierzytelnienie tylko jednym z wybranych mechanizmów uwierzytelnienia?
Odpowiedź nr 281:
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 27, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 282:
Załącznik nr.9 pkt. 3.6.5.q : Czy zamawiający akceptuję realizację powyższych podpunktów poprzez dostępny w GUI formularz, w którym użytkownik będzie mógł wpisać adres URL? Po odczytaniu adresu URL System inspekcji ruchu wykona zapytanie do serwera DNS i na podstawie adresu IP umieszczonego w odpowiedzi zwróci użytkownikowi informację o kategoryzacji. Przekształcenie adresu IP na kategorię odbywać się będzie na podstawie statycznie zdefiniowanej tablicy zawierającej pary "adres IP - kategoria".
Odpowiedź nr 282:
Zamawiający nie akceptuje realizacji powyższych punktów poprzez dostępny w GUI formularz. Zmawiający wymaga, aby sprawdzenie opisane w punkcie 3.6.5 lit. q) Szczegółowego opisu przedmiotu zamówienia odbywało się automatycznie i przezroczyście dla użytkownika końcowego sieci OSE.

Pytanie nr 283:
Punkt 3.6.2 / 3.7.2 (e) określa dwa tryby pracy systemu NGFW, przy czym nakłada dodatkowy wymóg w postaci nie wprowadzania segmentacji na osobne domeny kolizyjne w sensie Ethernet/CSMA
O ile niektóre dostępne na rynku rozwiązania wprowadzają mechanizm określany „virtual wire" (lub „bump-in-the-wire"), tworząc niskopoziomowe połączenie pary (i wyłącznie pary, co de facto nie wypełnia wymagań tego punktu) interfejsów, o tyle nie jest możliwe dla żadnego aktywnego urządzenia sieciowego uzyskanie opisanego zjawiska. Każde urządzenie siłą rzeczy musi wprowadzać podział na domeny kolizyjne w sensie Ethernet/CSMA, chyba że zapewnia galwaniczne połączenie interfejsów, a jego interfejsy pracujące w trybie half-duplex (co sprowadza jego funkcję do koncentratora sieciowego, hub'a). Proponujemy usunąć ten wymóg, ponieważ nie moze być spełniony przez żadne dostępne na rynku urządzenie, w szczególności dysponujące wymaganymi w zapytaniu typami interfejsów.
Dodatkowo warto w naszej opinii uporządkować nazewnictwo trybów pracy systemu, bowiem o ile w omawianym punkcie tryb przełącznika i tryb transparentny są używane zamiennie, o p. (l) sugeruje obecność trzech trybów (transparentny, L2, L3). Proponujemy ujednolicenie do dwóch trybów: przełącznika (L2, transparentny) i routera (L3, routed).
Odpowiedź nr 283:
Zamawiający informuje, ze dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 25, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 284:
Punkty 3.6.2 / 3.7.2 (e), (l) i (t) wprowadzają wymogi związanie z logicznym podziałem urządzeń oraz trybami pracy poszczególnych instancji, w szczególności określają iż rozwiązania NGFW muszą zapewniać:

- Możliwość podziału na wirtualne instancje (co najmniej 5 – tylko dla trybu routed)
- Mozliwość uruchomienia więcej niz jednej tablicy routingu w pojedynczej instancji
- Możliwość pracy w trybach przełącznika (L2, transparentnym) i routera (L3, routed)
- Możliwość określenia trybu pracy per interfejs

W naszej opinii są to wymagania nieco nadmiarowe i redundantne, w szczególności biorąc pod uwagę architekturę węzłów sieci OSE.
Proponujemy potraktowanie mozliwości uruchomienia więcej niż jednej tablicy routingu w pojedynczej instancji jako opcjonalną (ew. alternatywną do obsługi wielu instancji).
Odpowiedź nr 284:
Pkt 3.6.2 / 3.7.2 lit. l) Szczegółowego opisu przedmiotu zamówienia
Dla Zmawiającego tryby pracy nie są tożsame. W trybie transparentnym nie występuje mac lerning.
Zamawiający podtrzymuje dotychczasowe brzmienie zapisów Zapytania ofertowego.
Pkt 3.6.2 / 3.7.2 lit. e) Szczegółowego opisu przedmiotu zamówienia
Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 25, opublikowana w piśmie z dnia 18.12.2018 r.
3.6.2 / 3.7.2 lit. t) Szczegółowego opisu przedmiotu zamówienia
Zamawiający dopuszcza separację ruchu jedynie na poziomie wirtualnych firewalli (w ramach wirtualnych firewalli nie musi być wsparcia dla VRF).

Zamawiający dokonał zmiany zapisów - patrz zmiana nr 28, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 285:

Punkty 3.4 (g) wymaga mozliwości uwierzytelniania administratorów za pomocą bazy lokalnej i z wykorzystaniem dwóch z wymienionych mechanizmów: RADIUS lub TACACS+ lub SAML

Mając na uwadze, że:

- SAML jest nie tyle protokołem uwierzytelnienia (rozumianym jako mechanizm komunikacji między urządzeniem uwierzytelniającym a katalogiem użytkowników), co mechanizmem obsługi jednokrotnego uwierzytelnienia (wymagającym zastosowania w procesie uwierzytelnienia dodatkowego protokołu typu RADIUS lub LDAP),
- TACACS+ jest protokołem który powstał (opracowany przez ....[1]) głównie w celu bardziej granularnej kontroli dostępu do interfejsów terminalowych i w stosunku do RADIUSa nie wykazuje istotnej przewagi przy uwierzytelnianiu dostępu do graficznych interfejsów zarządzania,
- aktualnie coraz więcej katalogów uzytkowników wykorzystuje interfejsy LDAP,

nasze rozwiązania nie obsługują w pełnym zakresie mechanizmów SAML oraz TACACS+ (tylko dla dostępu do CLI urządzeń). Proponujemy zatem zastąpienie wymogu SAML obsługą LDAP lub dodanie LDAP jako kolejnego mechanizmu. Nalezy przy tym zauważyć, że w procesie RFQ w odpowiedzi na jedno z pytań została dopuszczona możliwość uwierzytelniania za pomocą RADIUS i LDAP.

Odpowiedź nr 285:

Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 27, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 286:

Punkty 3.6.2 (p), (q), (r) określają zbiór funkcjonalności związanych z autoryzacją użytkowników i administratorów.

W procesie konsultacji przed ogłoszeniem postępowania zakupowego zrezygnowano z mechanizmów związanych z uwierzytelnianiem uzytkowników w systemie NGFW (uwierzytelnianie ma wedle naszej wiedzy mieć miejsce w innych miejscach OSE), o czym świadczy m.in. fakt usunięcia wymagań związanych z obsługą portalu uwierzytelniającego oraz zapisy punktu 3.10.1. Mając to na uwadze, obecność częściowych wymagań związanych z uwierzytelnianiem użytkowników wydaje się nie mieć zastosowania. Dodatkowo, mając na uwadze fakt, że wymóg obsługi złożonych polityk uwierzytelniania wieloskładnikowego dotyczy wyłącznie urządzeń NGFW mozna z dużym prawdopodobieństwem przyjąć, ze mechanizm nie będzie w praktyce wykorzystywany – jedynym komponentem w którym tego typu polityki wydają się być uzasadnione jest moduł dostępu zdalnego (SSL VPN), przy czym właściwsze było by ewentualne wprowadzenie takiego rozwiązania na poziomie systemu zarządzania tozsamością, obejmującego wszystkie komponenty systemu. Dodatkowo wymagania te są redundantne w stosunku do określonych w części ogólnej. Proponujemy zatem usunięcie nadmiarowych wymagań, ew. dostosowanie ich do wymagań określonych w p. 3.10.1, pozostawiając jedynie wymagania odnośnie zawartości polityk kontroli dostępu.

Odpowiedź nr 286:

Zamawiający podał wymagania w zakresie uwierzytelniania użytkownika w punktach 3.6.2 i 3.7.2 lit. p), q) i r) Szczegółowego opisu przedmiotu zamówienia (SOPZ). Zgodnie z zapisem w punkcie 3.10.1 SOPZ Zamawiający w przyszłości może wykorzystać tozsamość na urządzeniach NG Firewall.

Zamawiający informuje, ze modyfikuje treść Zapytania ofertowego – patrz zmiana nr 87.

Pytanie nr 287:

Punkt 3.4 (u) określa wymagania w zakresie tworzenia kopii zapasowej konfiguracji.

Kopie zapasowe konfiguracji urządzeń są oczywiście niezbędne w zakresie koniecznym do jej odtworzenia w przypadku awarii, niemniej narzucanie zarówno mechanizmu transportu, jak tez formatu kopii nie wydaje się być konieczne. Proponujemy usunięcie tych narzutów.

[1] Nazwa usunięta przez Zamawiającego

Przy takiej skali projektu modyfikacja konfiguracji przez korektę kopii konfiguracji i jej re-aplikację na urządzeniu nie jest mechanizmem optymalnym i powinno być dopuszczone wyłącznie jako funkcjonalność opcjonalna przy braku lepszych alternatyw, takich jak wykorzystanie interfejsów API, SNMP czy CLI. Kopia konfiguracji ma zatem wyłącznie rolę awaryjną.

Odpowiedź nr 287:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 30.

Pytanie nr 288:

Punkt 3.6.2 / 3.7.2 (j) określa m.in. wymagania w zakresie zapewnienia mechanizmów zarządzania pasmem w sieci.

Zgodnie z opisem architektury OSE (w szczególności punkt 2.3.3.2) głównym punktem egzekucji polityk QoS w sieci OSE będą urządzenia agregacyjne, co jest zgodne z dobrymi praktykami – mechanizmy te (w szczególności egzekucja polityk) powinny być realizowane w miejscach gdzie mamy do czynienia z agregacją wielu połączeń i potencjalnym wystąpieniem nadsubskrypcji ruchu.

Ruch, który trafi do węzłów bezpieczeństwa siłą rzeczy powinien być już odpowiednio sklasyfikowany, ew. ograniczony i dostosowany do wymogów polityk zarządzania pasmem, a co za tym idzie funkcjonalności z nimi związane nie wydają się niezbędne na poziome urządzeń NGFW – zarówno z punktu widzenia niepotrzebnego dodatkowego ich obciążenia, jak też miejsca w sieci. Warto przy tym zaznaczyć, iz pozostałe komponenty znajdujące się w ścieżce ruchu węzłach bezpieczeństwa (ADC, SSL) nie mają określonych wymagań w tym zakresie, więc i tak niemożliwe będzie uzyskanie kontroli QoS w całej ścieżce. Proponujemy usunięcie tego wymagania, ew. pozostawienie tylko wymagań w zakresie obsługi oznaczeń DiffServ i ograniczania pasma).

Odpowiedź nr 288:

Zamawiający informuje, że dokonuje zmiany zapisów Zapytania ofertowego - patrz zmiana nr 31, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 289:

Punkt 3.6.2 / 3.7.2 (o) określa wymagania w zakresie ochrony przed atakami DoS, w tym z wykorzystaniem mechanizmu skanowania portów

Wykrywanie przez NGFW nadmiernych przepływów związanych z próbami ataków typu DoS jest oczywiście funkcjonalnością pożądaną, jednak w przypadku zdarzeń związanych z rekonesansem sieci, w szczególności skanowaniem portów taki atak z reguły nie ma miejsca. Zachowanie większości skanerów portów nie ma charakteru nadmiernego przepływu (flood), w związku z czym ich wykrycie / blokowanie jest efektywniejsze nie w mechanizmie anty-DoS, ale w mechanizmie IPS.

Proponujemy zatem usunięcie z tego punktu zapisu dotyczącego skanowania portów, ew przeniesienie go do części IPS (np. 3.6.2.2 / 3.7.2.2 (d)).

Odpowiedź nr 289:

Tak, Zamawiający dopuszcza taką sytuację, aby aktywność np. skanowania portów była blokowana przez IPS.

Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 26, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 290:

Punkt 3.6.2.3 / 3.7.2.3 (f) określa wymóg obsługi analizy heurystycznej przy wykrywaniu aplikacji.

Obecność tego wymogu w kontekście funkcjonalności kontroli aplikacji spełnia w naszej opinii tylko jeden z liczących się na rynku dostawców systemów NGFW. Prosimy o usunięcie zapisów *„i analizę heurystyczną"* oraz *„protokoły tunelowania i szyfrowania"*.

Odpowiedź nr 290:

Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 29, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 291:

Punkt 3.6.2.2 / 3.7.2.2 (e) określa wymóg dla mechanizmu wykrywania anomalii w ruchu sieciowym.

Mechanizmy wykrywania anomalii jest dość popularnym mechanizmem w rozwiązaniach NGWF, przy czym przyjmującym z reguły formy wykrywania anomalii protokołów bądź wykrywania anomalii za pomocą mechanizmów wolumetrycznych.
Opisany sposób implementacji jest w naszej opinii dość charakterystyczny dla jednego z dostawców rozwiązań NGFW, a ponadto mało efektywny przy zastosowaniu w architekturze OSE z kilku powodów. Po pierwsze – mając na uwadze sposób dystrybucji ruchu w węźle bezpieczeństwa, pojedyncze urządzenie nigdy nie będzie miało oglądu na kształt całości ruchu z danej podsieci czy szkoły, a co za tym idzie zbudowanie wzorca będzie nieefektywne i niemiarodajne. Po drugie – propagacja złośliwego oprogramowania czy skanowanie podsieci będą miał miejsce głównie w sieciach wewnętrznych, poza zasięgiem mechanizmów analitycznych NGFW. Po trzecie – oba typy zagrożeń mogą być wykrywane za pomocą innych mechanizmów (AV, IPS).
Efektywna analiza anomalii w ruchu sieciowym wymaga od mechanizmu analitycznego akwizycji danych metrycznych z wielu punktów różnych miejsc w sieci, w szczególności położonych możliwie blisko potencjalnych źródeł zagrożeń – takie funkcjonalności są zatem domeną narzędzi analitycznych takich jak Stealthwatch, Darktrace czy Flowmon Ich realizacja na poziomie rozwiązań NGFW jest nieoptymalna i nieefektywna.
Proponujemy wykreślenie wymagania, przynajmniej w części *„wzorcem, mające na celu wykrycie takich zagrożeń jak np. propagacja złośliwego oprogramowania lub skanowanie podsieci"*.

Odpowiedź nr 291:

Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 10, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 292:

Punkt 3.6.2 / 3.7.2 (v) określa wymagania dla możliwości dostosowania powiadomień.
Mając na uwadze funkcjonalności pełnione przez system NGFW w przyjętej architekturze ilość powiadomień wyświetlanych użytkownikom będzie nikła. Większość powiadomień w takich systemach dotyczy mechanizmów filtrowania URL, które będą realizowane na poziomie SWG. Transmisje plików blokowane przez funkcjonalności AV nie będą umożliwiały generowania powiadomienia, bo dotyczą tylko ruchu innego niż HTTP/HTTPS. Zdarzenia blokowane przez IPS również generalnie nie generują komunikatów dla użytkowników, co sprowadza ich ew. wyświetlanie właściwie tylko do funkcjonalności kontroli aplikacji w ramach ruchu HTTP/HTTPS.
Proponujemy zatem modyfikację wymagania przez usunięcie treści od *„ w szczególności ..."*

Odpowiedź nr 292:

Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 7 i 8, opublikowane w piśmie z dnia 18.12.2018 r.

Pytanie nr 293:

Punkt 3.7.8 określa wymagania na system zarządzający
Na wstępie należy zaznaczyć, iż system zarządzający infrastruktury bezpieczeństwa będzie de facto zestawem systemów obsługujących poszczególne elementy (ADS/SSL, NGFW, DNS, ...), których specyfika może znacząco różnić się od siebie. Wymagania określone dla systemu zarządzania są stosunkowo generyczne, opisujące „klasyczny" system zarządzania oparty na tworzeniu swoistej nakładki na poszczególne urządzenia, komunikujący się z nimi przez typowe interfejsy typu SNMP.
W przypadku rozwiązania .....[2] Firepower system zarządzania (Firepower Management Center – FMC) ma nieco inny charakter, który można porównać o modelu znanego z implementacji rozwiązań klasy SDN. W przypadku jego wykorzystania (alternatywą jest możliwość „klasycznego", bezpośredniego zarządzania poszczególnymi urządzeniami) przejmuje on całość funkcji zarządczych, kontrolnych i raportujących, gwarantując spójność konfiguracji i polityk bezpieczeństwa. Przy tym zachowane są interfejsy diagnostyczne (SSH/HTTPS) dla poszczególnych urządzeń, niemniej całość konfiguracji jest dokonywana przez FMC (CLI, GUI, API).
Specyfika tego rozwiązania powoduje, że pomimo zachowania funkcjonalności określonych w postępowaniu, nie spełnia od wszystkich wymagań implementacyjnych.

[2] Nazwa usunięta przez Zamawiającego

W szczególności:

- Punkt (d) nakłada konieczność zapewnienia integracji przez modyfikację plików płaskich – w przypadku dostępnych interfejsów programistycznych (API) i klasycznych interfejsów zarządzania (CLI, GUI) taka funkcjonalność nie wydaje się niezbędna. Powinna być traktowana raczej jako gorsza alternatywa w przypadku braku innych interfejsów
- Punkt (e), (k) określa wymóg zbierania z urządzeń danych w formie m.in. SNMP trap. W przypadku rozwiązania Firepower to FMC ewentualnie generuje trap SNMP, podczas gdy zdarzenia i alarmy z urządzeń zbiera innymi mechanizmami (urządzenia są przy tym w stanie wysyłać zdarzenia w formacie syslog bezpośrednio do SIEM)
- FMC nie monitoruje warstwy sprzętowej – mozliwe jest dodanie osobnego modułu oprogramowania który zapewni te funkcjonalności
- Punkt (g) – FMC nie ma możliwości eksportu danych o dostępności systemów do PDF (mozna go wyświetlić w GUI)

Proponujemy modyfikację wymagań w zakresie powyższych niezgodności.

Odpowiedź nr 293:

Zamawiający informuje, że dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 32, opublikowana w piśmie z dnia 18.12.2018 r.

Pytanie nr 294:

Rozwiązania DNS

Określona we wcześniejszych procesach, jak też testowana w projekcie pilotażowym funkcjonalność DNS skupiona była przede wszystkim na wsparciu systemów bezpieczeństwa (NGFW, SWG) w zakresie zapobiegania zagrożeniom. Wymagania określone w postępowaniu wydają się spychać tą rolę na drugi plan, podczas gdy na pierwszy wysuwa się funkcjonalność serwera DNS. Efektem takiego rozszerzenia jest zmniejszenie w naszej opinii funkcjonalności traktowanej do tej pory jako priorytetowa i obniżenie jej jakości (wymagania nie określają na przykład pojemności baz reputacyjnych czy filtracji URL) kosztem funkcjonalności, które mogą być uzyskane innymi metodami (np. użyciem serwerów DNS NASK na potrzeby OSE). Uwzględniając wszystkie wymagania, w naszej opinii pozostaje jeden system je spełniający, stanowiący „klasyczne" rozwiązanie DNS/DNS firewall.

Proponujemy umożliwienie oferowania nowoczesnych systemów tej klasy opartych na rozwiązaniach hybrydowych, łączących mechanizmy osadzane w sieci wewnętrznej i mechanizmy chmurowe, gwarantujące znaczące zwiększenie skali, poprawę jakości baz danych i mechanizmów analitycznych oraz znaczące zmniejszenie czasu potrzebnego do reakcji na nowe zagrożenia.

W tym celu proponujemy modyfikację zapisów w następującym zakresie:

- Wykreślenie punktów (c), (d), (e), (f), (h), (i), (j), (k), (q) i zastąpienie ich bardziej elastycznymi wymaganiami typu:
    - *system powinien działać na rekordach DNS typu: A, AAAA, ANY, CNAME, PTR, SRV i TXT i umożliwiać współpracę z lokalnymi serwerami DNS*
    - *klasyfikacja zagrożeń powinna opierać się o mechanizmach uczenia maszynowego wykorzystujące globalnie zbierane informacje o domenach, adresach IP oraz systemach autonomicznych BGP (ASN)*
    - *dopuszczalne jest zastosowanie rozwiązania bazującego na urządzeniach instalowanych wewnątrz sieci lub na jej brzegu, jak też środowisk chmurowych – w takim przypadku rozwiązanie obejmuje wewnętrzne narzędzia umożliwiające przekierowywanie zapytań DNS pozwalających na szyfrowane przesyłanie zapytań, oraz odpowiedzi DNS od klienta do chmury, oraz z chmury do klienta*
- Modyfikację punktu (m) w zakresie treści w nawiasie
- Wykreślenie punktu (o) jako redundantnego funkcjonalnie z punktem (n) przy tym narzucającego wariant implementacyjny
- Modyfikacji punktu (p) w zakresie wykreślenia treści *„(NSDNAME i NSIP)", „z odpowiedzią NXDOMAIN", „z odpowiedzią NODATA"*

Odpowiedź nr 294:

Zamawiający pozostawia zapisy w dotychczasowym brzmieniu.

Pytanie nr 295:

Na koniec chciałbym zwrócić uwagę, iz wymagania wydajnościowe określone dla poszczególnych węzłów są istotnie wyższe od określonych podczas procesu RFQ. Wynika to zarówno z podniesionych wymagań odnośnie przepustowości, jak tez (a wręcz przede wszystkim) z bardzo znaczącej zmiany charakterystyki ruchu wzorcowego stanowiącego podstawę do wyskalowania rozwiązań. Na etapie RFQ ruch wzorcowy zakładał wykorzystanie ruchu złozonego z dużych pakietów (tylko 1518B), podczas gdy w aktualnym postępowaniu ruch wzorcowy jest zgodny z tzw. Simple IMIX (zdefiniowany przez dostawców generatorów ruchu sieciowego ponad dekadę temu). Pomijając fakt, iz powołanie się w tym przypadku na RFC 6985 nie ma większego sensu, jako ze wskazany rozkład pakietów nie wykorzystuje zadnej wielkości wymienionej w tym RFC (a co za tym idzie nie da się go zdefiniować genomem w nim określonym) ten krok prowadzi do znacznego (4x – 5x) zwiększenia wymagań wydajnościowych właściwie wszystkich elementów węzła. Fikcją jest przy tym przyjęcie założenia, iz średnia wielkość pakietu nie ma znaczenia dla skalowania wydajności. Wnioski takie można co prawda pochopnie wysnuć bazując np. na wynikach testów niektórych rozwiązań przeprowadzonych np. w przypadku tegorocznych testów organizacji NSS (dwa rozwiązania w testach przepustowości wydawały się utrzymywać maksymalną przepustowość dla dowolnej długości pakietu), jednak należy mieć na uwadze, że:

- jak określono w tym raporcie, test miał na celu wyłącznie zbadanie zdolności do przełączania ruchu, bez głębokiej jego inspekcji,
- test dotyczył wyłącznie ruchu UDP – z natury bezstanowego, a co za tym idzie w większości rozwiązań częściowo lub całkowicie pomijanego przy analizie.

Rozwiązania ....[3] Firepower posiadają mechanizmy pozwalające na inteligentne pominięcie zaufanych przepływów i uzyskanie w podobnych testach znacznie lepszych rezultatów, co nie zmienia faktu, iz wydajność wszystkich rozwiązań NGFW dostępnych na rynku w przypadku zastosowania głębokiej analizy w warstwach wyzszych (L4-7) będzie znacząco niższa od wydajności katalogowych, a co za tym idzie odpowiedzialnie konstruując ofertę konieczne jest znacząco wyższe wyskalowanie rozwiązań, zwiększając ich koszt.

Proponujemy modyfikację ujętego w zapytaniu rozkładu długości pakietów do stanu z RFQ lub dostosowanie go do ruchu obserwowanego w projekcie pilotazowym albo zgodnego z aktualnymi statystykami wielkości pakietów w Internecie (okolice 700B zgodnie z https://www.caida.org/data/passive/trace_stats/), co pozwoli na optymalny ekonomicznie dobór rozwiązań.

Odpowiedź nr 295:

Zamawiający informuje, ze dokonał zmiany zapisów Zapytania ofertowego - patrz zmiana nr 33, opublikowana w piśmie z dnia 18.12.2018 r.

II. Zgodnie z rozdziałem VII pkt 10 Zapytania ofertowego, Zamawiający dokonuje następujących zmian treści Zapytania ofertowego:

Zmiana nr 66

Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 Zapytania ofertowego, pkt 3.6.4 lit. a) i pkt 3.7.4 lit. a)

Było:

„Zaoferowane rozwiązania dla Systemu ADC muszą opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Application Delivery Controllers lub Gartner Market Guide for Application Delivery Controllers, lub analogicznych zestawieniach przygotowanych przez równowazne organizacje, przygotowanych w ciągu ostatnich trzech lat."

[3] Nazwa usunięta przez Zamawiającego

Po zmianie jest:
„Zaoferowane rozwiązania dla Systemu ADC muszą opierać się o firmy znajdujące w zestawieniach przygotowanych przez Gartnera dla kategorii Gartner Magic Quadrant for Application Delivery Controllers lub Gartner Market Guide for Application Delivery Controllers, lub analogicznych zestawieniach przygotowanych przez równoważne organizacje, przygotowanych w ciągu ostatnich trzech lat przed upływem terminu składania ofert."

Zmiana nr 67
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego, pkt 3.5. lit. c)

BYŁO:
„z wyłączeniem systemów:
-zarządzających elementami Infrastruktury bezpieczeństwa
-elementów Infrastruktury bezpieczeństwa, które będą tworzyć elementy Centralnego Węzła Bezpieczeństwa"

PO ZMIANIE JEST:
„z wyłączeniem systemów:
-zarządzających elementami Infrastruktury bezpieczeństwa
-elementów Infrastruktury bezpieczeństwa, które będą tworzyć elementy Centralnego Węzła Bezpieczeństwa
-elementów Węzła laboratoryjnego"

Zmiana nr 68
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego, pkt 3.6.4 lit. w) i pkt 3.7.4 lit. w)

BYŁO:
"System ADC musi posiadać funkcje przywiązywania sesji (Session persistence) do określonej ścieżku ruchu na podstawie konfiguracji przez Zamawiającego reguł wykorzystujących co najmniej następujące atrybuty:
Ø Cookie (hash, rewrite, custom, insert, passive)
Ø Adres źródła
Ø Identyfikator sesji SSL

Ø Adres docelowy
Ø Tworzonych przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 3.6.4 ppkt. m
Ø Badanie obciążenia poszczególnych nodów w klastrze pod względem obciążenia"

PO ZMIANIE JEST:
"System ADC musi posiadać funkcje przywiązywania sesji (Session persistence) do określonej ściezku ruchu na podstawie konfiguracji przez Zamawiającego reguł wykorzystujących co najmniej następujące atrybuty:
Ø Cookie (hash, rewrite, custom, insert, passive)
Ø Adres źródła
Ø Identyfikator sesji SSL
Ø Adres docelowy

Ø Tworzonych przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 3.6.4 ppkt. q
Ø Badanie obciązenia poszczególnych nodów w klastrze pod względem obciązenia"

Zmiana nr 69
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego

Zamawiający modyfikuje zapisy poprzez

a) dodanie do pkt 3.6.4 lit. ff) oraz pkt 3.7.4 lit. ff) zapisu w brzmieniu: „System ADC musi obsługiwać protokoły dynamicznego routingu BGP i OSPF"
b) dodanie do pkt 3.6.5 lit. s) oraz pkt. 3.7.7 lit. s) zapisu w brzmieniu: „System inspekcji ruchu SSL/TLS musi obsługiwać protokoły dynamicznego routingu BGP i OSPF."

Zmiana nr 70
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego

a) pkt 3.6.5 lit. k)

Zamawiający modyfikuje zapisy poprzez usunięcie pkt 3.6.5 lit k) w brzmieniu:

„System inspekcji ruchu SSL/TLS musi umozliwiać Zamawiającemu definiowanie wyjątków, od reguł określających jaki ruch podlega inspekcji, w oparciu o przygotowaną przez Wykonawcę statyczną listę zawierającą adresy URL z kategorii treści:
Ø Zdrowie Polskie Strony – strony placówek medycznych udostępniające dla klientów w Polsce usługi medyczne i prezentujące dla uzytkowników dane wrazliwe, takie jak np. wyniki badań
Ø Bankowość – strony instytucji finansowych przetwarzających, prezentujących i udostępniających dane wrażliwe uzytkowników, np. w postaci portali transakcyjnych umozliwiających na sprawdzanie stanu konta lub wykonywanie operacji finansowych takich jak np. przelewy
Zamawiający rezerwuje sobie prawo na dodanie do dwóch kategorii treści, które zostaną zdefiniowane na etapie Projektu Technicznego."

b) pkt 3.7.7 lit. k)

Zamawiający modyfikuje zapisy poprzez usunięcie pkt 3.7.7 lit k) w brzmieniu:

„System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu definiowanie wyjątków, od reguł określających jaki ruch podlega inspekcji, w oparciu o przygotowaną przez Wykonawcę statyczną listę zawierającą adresy URL z kategorii treści:
Ø Zdrowie Polskie Strony – strony placówek medycznych udostępniające dla klientów w Polsce usługi medyczne i prezentujące dla uzytkowników dane wrazliwe, takie jak np. wyniki badań
Ø Bankowość – strony instytucji finansowych przetwarzających, prezentujących i udostępniających dane wrazliwe użytkowników, np. w postaci portali transakcyjnych umożliwiających na sprawdzanie stanu konta lub wykonywanie operacji finansowych takich jak np. przelewy
Zamawiający rezerwuje sobie prawo na dodanie do dwóch kategorii treści, które zostaną zdefiniowane na etapie Projektu Technicznego."

Zmiana nr 71
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.2 (nagłówek)

BYŁO:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System NG Firewall działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa".”

PO ZMIANIE JEST:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System NG Firewall działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2. „ Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa".”

Zmiana nr 72
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.2 .2(nagłówek)

BYŁO:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność IPS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall."

PO ZMIANIE JEST:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność IPS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall."

Zmiana nr 73
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.2.3 (nagłówek)

BYŁO:
„W ramach wdrozonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność Kontroli aplikacji (udostępnianych poprzez sieć Internet) działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall."

PO ZMIANIE JEST:
„W ramach wdrozonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność Kontroli aplikacji (udostępnianych poprzez sieć Internet) działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG Firewall."

Zmiana nr 74
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.4 (nagłówek)

BYŁO:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System ADC działał w skali

całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa”.”

PO ZMIANIE JEST:
„W ramach wdrozonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby System ADC działał w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa”.”

Zmiana nr 75
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.5 (nagłówek)

BYŁO:
„W ramach wdrozonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie ponizsze wymagania. Zamawiający wymaga aby funkcjonalność SSL VPN działała dla liczby użytkowników określonej w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa”.”

PO ZMIANIE JEST:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie ponizsze wymagania. Zamawiający wymaga aby funkcjonalność SSL VPN działała dla liczby użytkowników określonej w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa”.”

Zmiana nr 76
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.6 (nagłówek)

BYŁO:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie ponizsze wymagania. Zamawiający wymaga aby Funkcjonalność WAF działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa”. Zamawiający zakłada realizację funkcjonalności Web application Firewall (WAF) na Systemie ADC lub jako dedykowane Urządzenie typu appliance.”

PO ZMIANIE JEST:
„W ramach wdrozonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby Funkcjonalność WAF działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa”. Zamawiający zakłada realizację funkcjonalności Web application Firewall (WAF) na Systemie ADC lub jako dedykowane Urządzenie typu appliance.”

Zmiana nr 77
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.7 (nagłówek)

BYŁO:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie ponizsze wymagania. Zamawiający wymaga aby funkcjonalność inspekcji ruchu SSL/TLS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa”. Zamawiający określa, że poprzez inspekcję ma na myśli deszyfrowanie i ponowne szyfrowanie ruchu SSL/TLS sklasyfikowanego na podstawie określonych przez Zamawiającego reguł.”

PO ZMIANIE JEST:
„W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie poniższe wymagania. Zamawiający wymaga aby funkcjonalność inspekcji ruchu SSL/TLS działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3.2 „Wymagania wydajnościowe na Centralne Węzły Bezpieczeństwa". Zamawiający określa, ze poprzez inspekcję ma na myśli deszyfrowanie i ponowne szyfrowanie ruchu SSL/TLS sklasyfikowanego na podstawie określonych przez Zamawiającego reguł."

Zmiana nr 78
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, pkt. 3.8

BYŁO:
"Węzeł laboratoryjny opisany ponizej musi odzwierciedlać pod kątem funkcjonalnym Infrastrukturę bezpieczeństwa pracującą w Regionalnym Węźle Bezpieczeństwa i Centralnym Węźle Bezpieczeństwa. Wydajność Węzła laboratoryjnego musi być zgodna z tabelą podaną w rozdziale 3.3 „Skalowanie elementów Infrastruktury bezpieczeństwa", z zachowaniem funkcjonalności uruchomionych w Regionalnym Węźle Bezpieczeństwa i Centralnym Węźle Bezpieczeństwa."

PO ZMIANIE JEST:
"Węzeł laboratoryjny opisany ponizej musi odzwierciedlać pod kątem funkcjonalnym Infrastrukturę bezpieczeństwa pracującą w Regionalnym Węźle Bezpieczeństwa i Centralnym Węźle Bezpieczeństwa. Wydajność Węzła laboratoryjnego musi być zgodna z tabelą podaną w rozdziale 3.3.2 „Wymagania wydajnościowe na Węzeł laboratoryjny", z zachowaniem funkcjonalności uruchomionych w Regionalnym Węźle Bezpieczeństwa i Centralnym Węźle Bezpieczeństwa. "

Zmiana nr 79
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, pkt. 3.8.3

BYŁO:
"Zamawiający dostarczy oprogramowanie identyczne z oferowanym Systemem zarządzającym (mozliwe jest nałożenie ograniczeń wydajnościowych) wraz z licencją umożliwiającą wykorzystanie tego oprogramowania wyłącznie do celów rozwojowo-testowych (bez prawa do wykorzystania w sieci eksploatowanej komercyjnie).
Oferowane oprogramowanie (wraz z licencją) musi zapewniać mozliwość współpracy z oferowanym testowym środowiskiem fizycznym oraz współpracy z systemami testowymi OSS/BSS Zamawiającego wyszczególnionymi w pkt 3.10."

PO ZMIANIE JEST:
"Wykonawca dostarczy oprogramowanie identyczne z oferowanym Systemem zarządzającym (mozliwe jest nałożenie ograniczeń wydajnościowych) wraz z licencją umożliwiającą wykorzystanie tego oprogramowania wyłącznie do celów rozwojowo-testowych (bez prawa do wykorzystania w sieci eksploatowanej komercyjnie).
Oferowane oprogramowanie (wraz z licencją) musi zapewniać możliwość współpracy z oferowanym testowym środowiskiem fizycznym oraz współpracy z systemami testowymi OSS/BSS Zamawiającego wyszczególnionymi w pkt 3.10."

Zmiana nr 80
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego, pkt 3.6.4 lit. o)

a) pkt 3.6.4 lit. o)

BYŁO:
"System ADC musi umożliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI i CN) poprzez współpracę z Systemem DNS."

PO ZMIANIE JEST:
"System ADC musi umozliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI lub SNI i CN) poprzez współpracę z Systemem DNS. Alternatywnie Zamawiający dopuszcza zastosowanie wewnętrznej bazy kategoryzacji dostarczonej przez producenta ADC."

b) pkt 3.6.5 lit. q) i pkt 3.7.7 lit. q)

BYŁO:
"System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI i CN) poprzez współpracę z Systemem DNS.."

PO ZMIANIE JEST:

c) " System inspekcji ruchu SSL/TLS musi umożliwiać Zamawiającemu sprawdzanie kategoryzacji adresu URL zawartego w certyfikacie (pola SNI lub SNI i CN) poprzez współpracę z Systemem DNS."**Pkt. 3.2.2**

BYŁO:
„Cały ruch (100%) od CPE, po przejściu przez Węzeł agregacyjny, przechodzi przez System ADC, który dokonuje deszyfracji SSL wewnętrznie lub z wykorzystaniem Urządzeń dedykowanych. Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI i CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii do jakiej nalezy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS. Wykonawca na etapie realizacji przedmiotu zamówienia jest zobowiązany do konfiguracji Systemu ADC i Systemu DNS w sposób umozliwiający wykonanie tej funkcjonalności."

PO ZMIANIE JEST:
„Cały ruch (100%) od CPE, po przejściu przez Węzeł agregacyjny, przechodzi przez System ADC, który dokonuje deszyfracji SSL wewnętrznie lub z wykorzystaniem Urządzeń dedykowanych. Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI lub CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii do jakiej nalezy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS. Wykonawca na etapie realizacji przedmiotu zamówienia jest zobowiązany do konfiguracji Systemu ADC i Systemu DNS w sposób umożliwiający wykonanie tej funkcjonalności."

Zmiana nr 81
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego, pkt 3.7.5 lit. b)

BYŁO:
„Funkcjonalność SSL VPN musi umozliwiać Zamawiającemu na definiowanie polityki dostępu poprzez graficzny edytor, który pozwoli Zamawiającemu wybierać konkretne obiekty konfiguracyjne (elementy uwierzytelnienia, konfiguracji dostępu, dostępnych zasobów, itp.) oraz najczęstsze powtarzające się konfiguracje kopiować do makr."

PO ZMIANIE JEST:
„Funkcjonalność SSL VPN musi umożliwiać Zamawiającemu na definiowanie polityki dostępu poprzez graficzny edytor, który pozwoli Zamawiającemu wybierać konkretne obiekty konfiguracyjne (elementy uwierzytelnienia, konfiguracji dostępu, dostępnych zasobów, itp.) oraz najczęstsze powtarzające się konfiguracje kopiować do makr, alternatywnie definiowanie makr i ich sekwencji w sposób tekstowy."

Zmiana nr 82
Wzór umowy stanowiący Załącznik nr 2 do Zapytania ofertowego, §4 ust. 11

BYŁO:
„W przypadku dokonania przez Zamawiającego warunkowego Odbioru Wstępnego, Zamawiający nie jest uprawniony do dochodzenia kar umownych za opóźnienie we Wdrożeniu przez okres wyznaczony na usunięcie Błędów i Wad wymienionych w. Protokole."

PO ZMIANIE JEST:
„W przypadku dokonania przez Zamawiającego warunkowego Odbioru Wstępnego, Zamawiający nie jest uprawniony do dochodzenia kar umownych za opóźnienie we Wdrożeniu za okres wyznaczony na usunięcie Błędów i Wad wymienionych w Protokole."

Zmiana nr 83
Wzór umowy stanowiący Załącznik nr 2 do Zapytania ofertowego, §9 ust. 7

BYŁO:
"Stosowanie praw wynikających z udzielonej Gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady Urządzeń i/lub Oprogramowania. Wykonawca zobowiązany jest do zapewnienia usunięcia zgłoszonych przez Zamawiającego wad w ramach rękojmi w terminie wskazanym przez Zamawiającego."

PO ZMIANIE JEST:
"Stosowanie praw wynikających z udzielonej Gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady Urządzeń i/lub Oprogramowania. Wykonawca zobowiązany jest do zapewnienia usunięcia zgłoszonych przez Zamawiającego wad w ramach rękojmi w terminie wskazanym przez Zamawiającego, nie krótszym niz 7 dni".

Zmiana nr 84
Wzór umowy stanowiący Załącznik nr 2 do Zapytania ofertowego, §18 ust. 3

BYŁO:
„Obowiązek zachowania tajemnicy jest nieograniczony w czasie. Zwolnienie danej Strony z obowiązku zachowania tajemnicy jest mozliwe tylko za uprzednią pisemną zgodą drugiej Strony."

PO ZMIANIE JEST:
„Obowiązek zachowania tajemnicy trwa przez okres 5 lat od daty zakończenia Uomwy. Zwolnienie danej Strony z obowiązku zachowania tajemnicy jest możliwe tylko za uprzednią pisemną zgodą drugiej Strony."

Zmiana nr 85
Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego

Zamawiający modyfikuje zapisy poprzez dodanie punktu 3.4 lit. y) w brzmieniu:

„Infrastruktura bezpieczeństwa musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B."

Zmiana nr 86

Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego, część zapisu w pkt. 3.7.2 .1(nagłówek)

BYŁO:

„W ramach wdrozonej Infrastruktury bezpieczeństwa w Regionalnym Węźle Bezpieczeństwa muszą być spełnione wszystkie ponizsze wymagania. Zamawiający wymaga aby funkcjonalność AV działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG firewall. Zamawiający dopuszcza realizację tej funkcjonalności w sposób równoważny z wykorzystaniem dedykowanych Urządzeń lub jedynie w Węzłach Centralnych przy założeniu realizacji funkcjonalności AV dla wszystkich Użytkowników obsługiwanych przez dany Węzeł."

PO ZMIANIE JEST:

„W ramach wdrożonej Infrastruktury bezpieczeństwa w Centralnym Węźle Bezpieczeństwa muszą być spełnione wszystkie ponizsze wymagania. Zamawiający wymaga aby funkcjonalność AV działała w skali całego ruchu określonego dla danego węzła w punkcie 3.3. „Skalowanie elementów Infrastruktury bezpieczeństwa". Zamawiający wymaga realizacji danej funkcjonalności na Systemie NG firewall. Zamawiający dopuszcza realizację tej funkcjonalności w sposób równowazny z wykorzystaniem dedykowanych Urządzeń lub jedynie w Węzłach Centralnych przy założeniu realizacji funkcjonalności AV dla wszystkich Użytkowników obsługiwanych przez dany Węzeł."

Zmiana nr 87

Szczegółowy opis przedmiotu zamówienia stanowiący Załącznik nr 1 do Zapytania ofertowego oraz „Formularz zgodności z wymaganiami Zamawiającego" stanowiący Załącznik nr 9 do Zapytania ofertowego,

a) pkt. 3.4 lit. g)

BYŁO:

„Infrastruktura bezpieczeństwa musi zapewniać Zamawiającemu możliwość uwierzytelniania administratorów za pomocą bazy lokalnej i z wykorzystaniem dwóch z wymienionych mechanizmów: RADIUS lub TACACS+ lub LDAP lub SAML."

PO ZMIANIE JEST:

„Infrastruktura bezpieczeństwa musi zapewniać Zamawiającemu mozliwość uwierzytelniania administratorów z wykorzystaniem dwóch z wymienionych mechanizmów: RADIUS lub TACACS+ lub LDAP lub SAML."

b) Pkt. 3.6.2 lit. r) i pkt. 3.7.2 lit. r)

BYŁO:

„*Polityka kontroli dostępu musi precyzyjnie definiować prawa dostępu* Uzytkowników i administratorów do określonych usług sieci i musi być utrzymywana nawet, gdy osoba zmieni lokalizację i adres IP. W przypadku Użytkowników i administratorów pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. System NG Firewall musi umozliwiać Zamawiającemu realizację wszystkich powyższych funkcji w oparciu o lokalną bazę jak i poprzez integrację z zewnętrznym systemem zarządzania tożsamością."

PO ZMIANIE JEST:

„Polityka kontroli dostępu musi precyzyjnie definiować prawa dostępu Użytkowników i administratorów do określonych usług sieci i musi być utrzymywana nawet, gdy osoba zmieni lokalizację i adres IP. W przypadku Użytkowników i administratorów pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się równiez transparentnie. System NG Firewall musi umożliwiać Zamawiającemu realizację wszystkich powyższych funkcji poprzez integrację z zewnętrznym systemem zarządzania tożsamością."

Zmiana nr 88

Zapytanie ofertowe, Rozdział III

Zamawiający dodaje nowy pkt. 14 o następującej treści:

„W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".
W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne"."

Zmiana nr 89

Zapytanie Ofertowe, Rozdział X, pkt 6

BYŁO:

„Wykonawca, który otrzymał największą liczbę punktów w powyższym kryterium oceny ofert, nie podlega wykluczeniu oraz spełnia warunki udziału w postepowaniu, zostanie zaproszony do przeprowadzenia testów weryfikacyjnych oferowanego Systemu, o których mowa w Załączniku nr 12 do Zapytania ofertowego (zwanymi dalej „testami weryfikacyjnymi"). Wykonawca będzie zobowiązany, w terminie do 2 dni od dnia przesłania przez Zamawiającego zaproszenia, wskazać lokalizację, w której zostaną przeprowadzone testy weryfikacyjne, a w ciągu kolejnych 5 dni udostępnić upoważnionym pracownikom Zamawiającego laboratorium z zainstalowanym i skonfigurowanym, według wymagań Zamawiającego, oferowanym przedmiotem zamówienia, w zakresie określonym w Załączniku nr 12 do Zapytania ofertowego oraz pod nadzorem Zamawiającego przeprowadzić testy weryfikacyjne. Testy mają na celu sprawdzenie przez Zamawiającego zgodności zaoferowanego przez Wykonawcę rozwiązania z wymogami SOPZ. Wykonawca przeprowadzi testy weryfikacyjne wg Scenariusza testów weryfikacyjnych stanowiącego Załącznik nr 12 do Zapytania ofertowego. Zamawiający będzie potwierdzał, dla każdego testowanego scenariusza, zgodność otrzymanego wyniku z wynikiem wymaganym. Po zakończeniu testów Zamawiający przekaże Wykonawcy protokół z przeprowadzonych testów, zawierający informacje o wyniku testów. Wszystkie koszty realizacji testów weryfikacyjnych m.in. związane z zapewnieniem środowiska testowego, urządzeń pomiarowych czy zasobów ludzkich zaangazowanych w prowadzenie testów po stronie Wykonawcy będą pokrywane przez Wykonawcę. Koszty związane z uczestnictwem pracowników Zamawiającego w

przeprowadzeniu testów weryfikacyjnych, w tym przejazdy i pobyt w trakcie testów weryfikacyjnych w miejscu ich przeprowadzenia, będą pokrywane przez Zamawiającego."

PO ZMIANIE JEST:

„Wykonawca, który otrzymał największą liczbę punktów w powyższym kryterium oceny ofert, nie podlega wykluczeniu oraz spełnia warunki udziału w postepowaniu, zostanie zaproszony do przeprowadzenia testów weryfikacyjnych oferowanego Systemu, o których mowa w Załączniku nr 12 do Zapytania ofertowego (zwanymi dalej „testami weryfikacyjnymi"). Wykonawca będzie zobowiązany, w terminie do 4 dni od dnia przesłania przez Zamawiającego zaproszenia, wskazać lokalizację, w której zostaną przeprowadzone testy weryfikacyjne, a w ciągu kolejnych 10 dni udostępnić upoważnionym pracownikom Zamawiającego laboratorium z zainstalowanym i skonfigurowanym, według wymagań Zamawiającego, oferowanym przedmiotem zamówienia, w zakresie określonym w Załączniku nr 12 do Zapytania ofertowego oraz pod nadzorem Zamawiającego przeprowadzić testy weryfikacyjne. Testy mają na celu sprawdzenie przez Zamawiającego zgodności zaoferowanego przez Wykonawcę rozwiązania z wymogami SOPZ. Wykonawca przeprowadzi testy weryfikacyjne wg Scenariusza testów weryfikacyjnych stanowiącego Załącznik nr 12 do Zapytania ofertowego. Zamawiający będzie potwierdzał, dla kazdego testowanego scenariusza, zgodność otrzymanego wyniku z wynikiem wymaganym. Po zakończeniu testów Zamawiający przekaze Wykonawcy protokół z przeprowadzonych testów, zawierający informacje o wyniku testów. Wszystkie koszty realizacji testów weryfikacyjnych m.in. związane z zapewnieniem środowiska testowego, urządzeń pomiarowych czy zasobów ludzkich zaangazowanych w prowadzenie testów po stronie Wykonawcy będą pokrywane przez Wykonawcę. Koszty związane z uczestnictwem pracowników Zamawiającego w przeprowadzeniu testów weryfikacyjnych, w tym przejazdy i pobyt w trakcie testów weryfikacyjnych w miejscu ich przeprowadzenia, będą pokrywane przez Zamawiającego."

III. **Zamawiający informuje, że wraz z odpowiedziami na powyższe pytania zamieszcza tekst jednolity Zapytania ofertowego, uwzględniający wszystkie zmiany treści Zapytania, wprowadzone przez Zamawiającego pismami z dnia 27.11.2018 r., 18.12.2018 r., 20.12.2018 r., 21.12.2018 r. oraz 24.12.2018 r.**

IV. **Zamawiający informuje, iż termin składania ofert zostaje przesunięty na dzień 04.01.2019 r. do godz. 12:00.**

Powyższe informacje należy traktować jako integralną część Zapytania ofertowego.

P.O. DYREKTORA
NASK
Państwowy Instytut Badawczy
mgr inż. Krzysztof Silicki

podpis Zamawiającego